HOEPLI TECNICA PER LA SCUOLA

Luigi Lo Russo
Elena Bianchi

3 SISTEMI E RETI

Nuova Edizione **OPENSCHOOL**

Per l'articolazione INFORMATICA degli Istituti Tecnici settore Tecnologico

Edizione **OPENSCHOOL**

1	**LIBRO**DITESTO
2	**E-BOOK+**
3	RISORSE**ONLINE**
4	**PIATTAFORMA**

LIBRO IN CHIARO

HOEPLI

Sistemi e reti

LUIGI LO RUSSO ELENA BIANCHI

Sistemi e reti

Nuova Edizione OPENSCHOOL

Per l'articolazione Informatica
degli Istituti Tecnici settore Tecnologico

VOLUME 3

EDITORE ULRICO HOEPLI MILANO

Copyright © Ulrico Hoepli Editore S.p.A. 2017
Via Hoepli 5, 20121 Milano (Italy)
tel. +39 02 864871 – fax +39 02 8052886
e-mail hoepli@hoepli.it

www.hoepli.it

Tutti i diritti sono riservati a norma di legge
e a norma delle convenzioni internazionali

Presentazione

Il corso, in **tre volumi**, illustra le **tecniche di gestione e funzionamento** delle **reti locali e geografiche**, con particolare attenzione ai **protocolli TCP/IP** usati da Internet. Tratta inoltre i **servizi di routing** e le **problematiche di instradamento**. Un'ampia sezione riguarda la configurazione del sistema operativo Linux e dei comandi di Shell.

Il **volume 3**, nella **Nuova Edizione Openschool**, completa l'analisi dei livelli più alti della pila protocollare ISO/OSI con le applicazioni e i servizi di rete. È suddiviso in unità di apprendimento ed è strutturato in **quattro sezioni tematiche**:

- **strato applicativo**;
- **reti virtuali e reti wireless**;
- **sicurezza delle reti** (**tecniche di autenticazione con server Radius**, **tecniche crittografiche** per la protezione dei dati con esempi C++ e PHP, **sicurezza delle connessioni**, **reti private** e normativa sulla **privacy**);
- i **modelli client-server** (**architetture** client-server, **sistemi distribuiti**, sistema operativo **Windows Server**).

Rispetto all'edizione precedente la nuova edizione del volume 3 presenta **numerose e significative novità**:

- una **nuova unità** iniziale sullo strato applicativo;
- aggiunta di **nuove lezioni specifiche per il laboratorio**;
- **schede CLIL** a conclusione di ogni unità.

In particolare lo studio del livello di rete è stato inserito e ampliato rispetto alla precedente edizione, arricchendolo con numerose nuove esercitazioni pratiche laboratoriali, molte corredate di procedure guidate.

Ogni sezione è composta da unità di apprendimento suddivise in più lezioni. Ciascuna lezione ha una **struttura innovativa** e cerca di essere una reale guida per l'apprendimento; essa, infatti, risulta **essenziale nei contenuti, ma ricca di esempi**.

Metodologia e strumenti didattici

Le finalità e i contenuti dei diversi argomenti affrontati sono descritti dagli **obiettivi generali** e dalle indicazioni ***In questa lezione impareremo***; alla fine di ogni lezione, per lo studente sono presenti **esercizi**, anche **interattivi**, **di valutazione delle conoscenze** e **delle competenze** raggiunte, suddivisi in **domande a risposta multipla**, **a completamento** e **vero o falso**.

Caratteristiche della nuova edizione

La Nuova Edizione Openschool consente di:

- **scaricare gratuitamente il libro digitale arricchito (eBook+)** che permette in particolare di:
  - eseguire tutte le **esercitazioni** a risposta chiusa in modo **interattivo**;
  - scaricare gli **approfondimenti tematici**, le **lezioni** e i **laboratori integrativi**;
- disporre di ulteriori esercitazioni online utilizzabili a discrezione del docente per classi virtuali gestibili attraverso la **piattaforma didattica**.

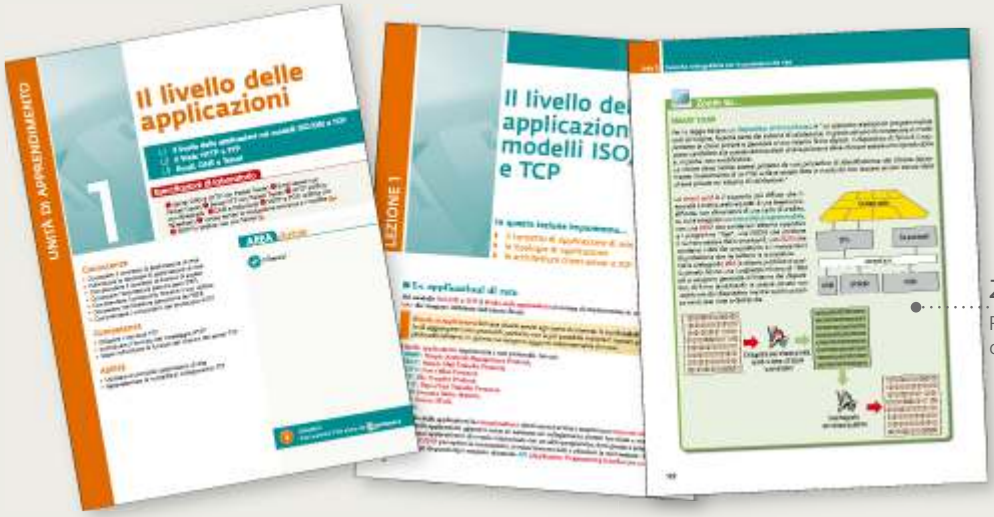
Aspetti caratterizzanti

- Testo pienamente in linea con le recenti indicazioni ministeriali in merito alle nuove **caratteristiche tecniche e tecnologiche dei libri misti e digitali** e al loro stretto coordinamento con la **piattaforma didattica**.
- Totale **duttilità di utilizzo in funzione delle scelte didattiche o dotazioni tecnologiche**:
  - il libro cartaceo consente di svolgere lezioni complete e attività di laboratorio;
  - l'eBook+, le risorse online e la piattaforma offrono il pieno supporto per una didattica multimediale, a discrezione delle scelte del docente.
- **Lezioni autoconclusive** ricche di esempi ed esercizi, adatte a essere svolte in una lezione o al massimo due.
- **Teoria ridotta al minimo per privilegiare l'aspetto pratico**.

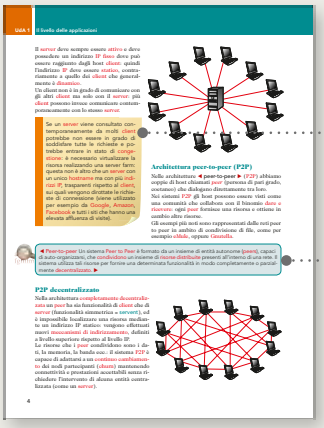
Materiali online hoepliscuola.it

Sul sito www.hoepliscuola.it sono disponibili numerose risorse online. In particolare, per lo studente: **approfondimenti**, utili integrazioni del testo e un numero elevato di **esercizi** sia per il **recupero e il rinforzo sia per l'approfondimento** degli argomenti trattati. Per il docente, una sezione riservata presenta alcune **unità didattiche per l'approfondimento** delle tematiche affrontate e un insieme di **schede aggiuntive** per la verifica dei livelli di apprendimento degli studenti. Materiali ed esercizi possono essere usati anche per creare attività didattiche fruibili tramite la piattaforma didattica accessibile dal sito.

Struttura dell'opera



ZOOM SU...
Piccole sezioni di approfondimento

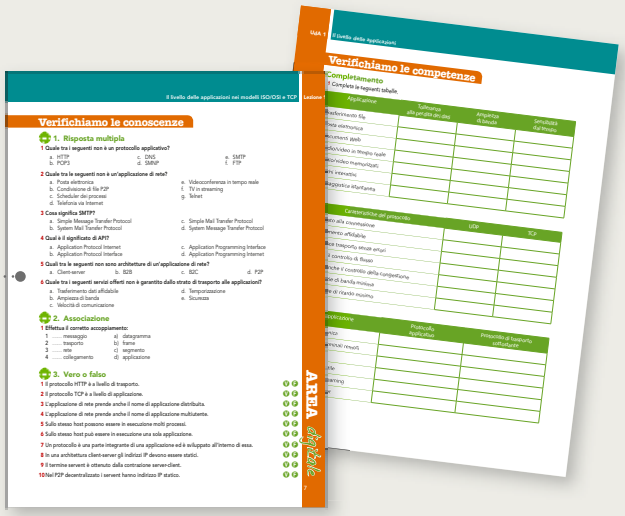


OSSERVAZIONI
Un aiuto per comprendere e approfondire

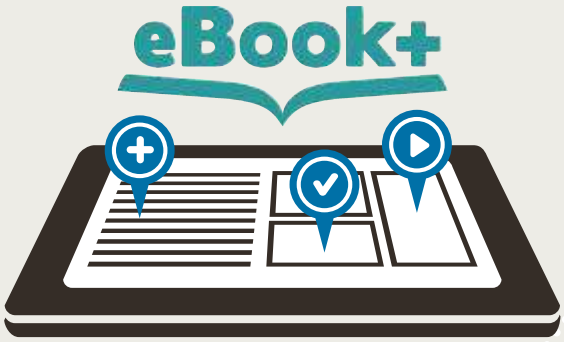
DEFINIZIONI
Spiegazione dei principali termini, delle funzioni e dei concetti trattati nel testo

LABORATORI
Per il rafforzamento dei concetti assimilati, attraverso esercitazioni operative

CLIL
Uno strumento di riepilogo in lingua inglese dei principali termini e concetti affrontati nell'unità

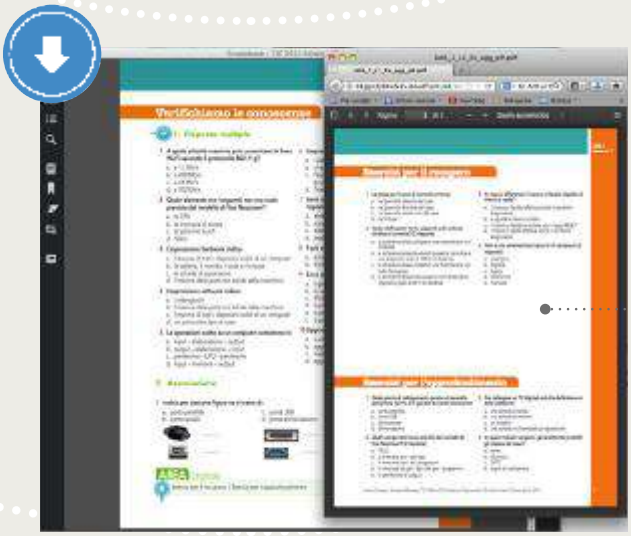


ESERCIZI
Ampia sezione di esercizi per la verifica delle conoscenze e delle competenze

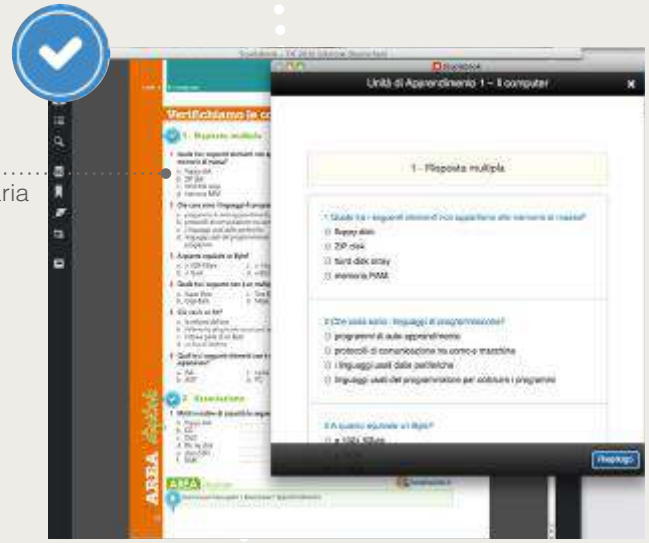


L'eBook+ riproduce le pagine del libro di testo in versione **digitale** e **interattiva**. È utilizzabile su tablet, LIM e computer e consente di **annotare**, **sottolineare** ed **evidenziare** il testo, salvando il proprio lavoro per poterlo consultare e sincronizzare sui diversi dispositivi. Apposite icone attivano i **contributi digitali integrativi**.

APPROFONDIMENTI
Contenuti, lezioni
e unità integrative



ESERCIZI AGGIUNTIVI
Esercizi per il recupero
e l'approfondimento



ESERCIZI

Esercizi interattivi di varia tipologia con funzione di autocorrezione

IMMAGINI E GALLERIE DI IMMAGINI

Per esemplificare e rappresentare visivamente i contenuti

LINK

Rimandi interni al volume per navigare agevolmente tra i contenuti

L'OFFERTA DIDATTICA **HOEPLI**

L'edizione **Openschool** Hoepli offre a docenti e studenti tutte le potenzialità di Openschool Network (ON), il nuovo sistema integrato di contenuti e servizi per l'apprendimento.

Edizione **OPENSCHOOL**

LIBRO DI TESTO

Il libro di testo è l'**elemento cardine** dell'offerta formativa, uno strumento didattico **agile** e **completo**, utilizzabile **autonomamente** o in combinazione con il ricco **corredo digitale** offline e online. Secondo le più recenti indicazioni ministeriali, volume cartaceo e apparati digitali **sono integrati in un unico percorso didattico**. Le espansioni accessibili attraverso l'eBook+ e i materiali integrativi disponibili nel sito dell'editore sono puntualmente richiamati nel testo tramite apposite icone.

eBOOK+

L'**eBook+** è la versione digitale e interattiva del libro di testo, utilizzabile su **tablet**, **LIM** e **computer**. Aiuta a comprendere e ad approfondire i contenuti, rendendo l'apprendimento più attivo e coinvolgente. Consente di leggere, annotare, sottolineare, effettuare ricerche e accedere direttamente alle numerose **risorse digitali integrative**.
➜ Scaricare l'eBook+ è molto **semplice**. È sufficiente seguire le istruzioni riportate nell'ultima pagina di questo volume.

RISORSE ONLINE

Il sito della casa editrice offre una ricca dotazione di **risorse digitali** per l'approfondimento e l'aggiornamento. Nella pagina web dedicata al testo è disponibile **MyBookBox**, il contenitore virtuale che raccoglie i materiali integrativi che accompagnano l'opera.
➜ Per accedere ai materiali è sufficiente registrarsi al sito **www.hoepliscuola.it** e inserire il codice coupon che si trova nella terza pagina di copertina.
Per il docente nel sito sono previste ulteriori risorse didattiche dedicate.

PIATTAFORMA DIDATTICA

La **piattaforma didattica** è un ambiente digitale che può essere utilizzato in modo duttile, a misura delle esigenze della classe e degli studenti. Permette in particolare di **condividere contenuti** ed **esercizi** e di partecipare a **classi virtuali**. Ogni attività svolta viene salvata sul **cloud** e rimane sempre disponibile e aggiornata. La piattaforma consente inoltre di consultare la versione online degli eBook+ presenti nella propria libreria.
➜ È possibile accedere alla piattaforma attraverso il sito **www.hoepliscuola.it**.

Indice

UNITÀ DI APPRENDIMENTO 1

Il livello delle applicazioni

L1 Il livello delle applicazioni nei modelli ISO/OSI e TCP

Le applicazioni di rete 2
Host 3
Architetture delle applicazioni di rete 3
Servizi offerti dallo strato di trasporto alle applicazioni 5
Verifichiamo le conoscenze 7
Verifichiamo le competenze 8

L2 Il Web: HTTP e FTP

Il World Wide Web 9
L'architettura del Web 10
Il protocollo HyperText Transfer Protocol (HTTP) 13
I cookies 16
HTTPS: Secure HyperText Transfer Protocol (cenni) 16
Il protocollo FTP 17
Verifichiamo le conoscenze 19

L3 Email, DNS e Telnet

Il servizio email 20
Invio e ricezione di posta elettronica 21
Il protocollo SMTP 23
Prelievo della posta: Post Office Protocol (POP3) 24
Protocollo IMAP 25
Nome simbolico e indirizzo IP 25
Telnet 28
Verifichiamo le conoscenze 32

Esercitazioni di laboratorio

1 Server DNS e HTTP con Packet Tracer 34
2 Email server con Packet Tracer 38
3 Server FTP con Packet Tracer 44
4 HTTP sniffing con Wireshark 49
5 DNS e Nslookup 55
6 SMTP e POP: sniffing con Wireshark 58
7 I proxy server, la navigazione anonima e i cookies
8 SMTP in pratica: uso con Telnet

Puoi scaricare i Lab. 7 e 8 anche da hoepliscuola.it

CLIL 63

UNITÀ DI APPRENDIMENTO 2

VLAN: Virtual Local Area Network

L1 Le Virtual LAN (VLAN)

Virtual LAN 66
Realizziamo una VLAN 67
Verifichiamo le conoscenze 71

L2 Il protocollo VTP e l'Inter-VLAN Routing

VLAN condivise su più di uno switch 72
Cisco VTP-VLAN Trunking Protocol 73
Inter-VLAN Routing 77
Verifichiamo le conoscenze 79
Verifichiamo le competenze 80

Esercitazioni di laboratorio

1 Realizziamo una VLAN con Packet Tracer 82
2 I comandi CLI per configurare la VLAN 86
3 VLAN e VTP con Packet Tracer 89

CLIL 93

UNITÀ DI APPRENDIMENTO 3

Tecniche crittografiche per la protezione dei dati

L1 La crittografia simmetrica

La sicurezza nelle reti 96
Crittografia 97
Crittoanalisi 98
Cifrari e chiavi 99
Il cifrario DES 100
3-DES 102
IDEA 103

AES ... 103
Limiti degli algoritmi simmetrici ... 106
Verifichiamo le conoscenze ... 107

L2 La crittografia asimmetrica
Generalità ... 108
RSA ... 113
Crittografia ibrida ... 117
Verifichiamo le competenze ... 119

L3 Certificati e firma digitale
I sistemi di autenticazione ... 120
Firme digitali ... 123
I certificati digitali ... 125
Riferimenti normativi ... 128
Verifichiamo le conoscenze ... 129

Esercitazioni di laboratorio
1 L'algoritmo di cifratura RSA in C++ ... 130
2 Un algoritmo di cifratura con PHP: MD5 ... 135
3 La crittografia in PHP: form sicuro con Crypt() ... 137
4 Crittografia in PHP con algoritmo Blowfish ... 143
5 Creazione di volumi criptati con VeraCrypt ... 147
6 La firma digitale con la carta CNS-TS ... 151
7 Algoritmi di cifratura in C++

Puoi scaricare il Lab. 7 anche da hoepliscuola.it

CLIL ... 163

AREA digitale
New directions in Cryptography, articolo completo

UNITÀ DI APPRENDIMENTO 4

La sicurezza delle reti

L1 La sicurezza nei sistemi informativi
La sicurezza dei dati ... 166
Sicurezza di un sistema informatico ... 169
Valutazione dei rischi ... 170
Principali tipologie di minacce ... 172
Sicurezza nei sistemi informativi distribuiti ... 173
La posta elettronica ... 175
Il protocollo S/MIME per la posta elettronica ... 176
Un software per la posta sicura: PGP ... 179
Verifichiamo le conoscenze ... 182

L2 La sicurezza delle connessioni con SSL/TLS
Generalità ... 183
Il protocollo SSL/TLS ... 184
Il funzionamento di TLS ... 186
Conclusioni ... 188
Verifichiamo le conoscenze ... 190

L3 Firewall, Proxy, ACL e DMZ
I firewall ... 191
Stateful inspection ... 196
Application proxy ... 197
DMZ ... 199
Verifichiamo le conoscenze ... 202

L4 Normativa sulla sicurezza e sulla privacy
Generalità
Giurisprudenza informatica
Il decreto 196/03 del 30 giugno 2003
L'articolo 98 del d.lgs. 30/2005
Legge 18 marzo 2008, n. 48,
Crimini informatici
Ultimi decreti e/o leggi
Conclusioni
Verifichiamo le conoscenze

Esercitazioni di laboratorio
1 Intercettare la password di posta elettronica con Sniff'em ... 203
2 Il pacchetto PGP Desktop ... 210
3 Realizziamo una VPN con Packet Tracer ... 226
4 Le Access Control List con Packet Tracer ... 229
5 Certificati digitali con Apache ... 237
6 Realizziamo una VPN P2P con Hamachi

Puoi scaricare la L4 e il Lab. 6 anche da hoepliscuola.it

CLIL ... 239

AREA *digitale*

Storia degli attacchi informatici

UNITÀ DI APPRENDIMENTO 5

Wireless e reti mobili

L1 Wireless: comunicare senza fili
Topologia 242
Lo standard IEEE 802.11 245
Il protocollo 802.11 legacy 245
Verifichiamo le conoscenze 249

L2 L'autenticazione nelle reti wireless
La sicurezza delle reti wireless 250
La crittografia dei dati 251
Wireless Protected Access (WPA-WPA2): generalità 254
Autenticazione 256
Verifichiamo le conoscenze 259

L3 La trasmissione wireless
Cenni sulle tecnologie trasmissive 260
Problemi nelle trasmissioni wireless 263
Struttura del frame 802.11 266
Il risparmio energetico nella trasmissione 269
Verifichiamo le conoscenze 270

L4 L'architettura delle reti wireless
Componenti di una rete wireless 271
Reti IBSS o modalità *ad hoc* 272
Servizi del Distribution System 278
Verifichiamo le conoscenze 280

L5 La normativa delle reti wireless
Generalità
Le disposizioni legali riguardanti le emissioni elettromagnetiche
L'obbligo di assunzione di misure minime di sicurezza in presenza di reti wireless
Reati informatici connessi al wireless
Leggi e decreti dell'ultimo decennio
Verifichiamo le conoscenze

Puoi scaricare la Lezione 5 anche da hoepliscuola.it

Esercitazioni di laboratorio

1 Access Point Lynksys con Packet Tracer 281
2 Server Radius con Packet Tracer 288
3 Controllare gli accessi wireless con Wireless Network Watcher 293

CLIL 296

UNITÀ DI APPRENDIMENTO 6

Modello client-server e distribuito per i servizi di rete

L1 Le applicazioni e i sistemi distribuiti
Le applicazioni distribuite 298
L'evoluzione delle architetture informatiche 299
Modelli di sistemi distribuiti: Windows 302
Verifichiamo le conoscenze 304

L2 Architetture dei sistemi Web
Architetture dei sistemi Web 305
Configurazione con due tier e unico host 306
Configurazione con tre tier e dual host 306
Configurazione con tre tier e server farm 307
Verifichiamo le conoscenze 311

L3 Amministrazione di una rete
Installazione dei componenti software di un client di rete 312
Configurazione dei protocolli di rete di un client 312
Amministrazione della rete 313
Servizi di directory 315
LDAP 316
DNS 317
Directory services in Windows 318
I domini 319
Verifichiamo le conoscenze 323

L4 Active Directory
Active Directory 324

I permessi di NTFS 327
Assegnazione dei permessi NTFS 330
I permessi di condivisione 334
Verifichiamo le conoscenze 335

L5 Il troubleshooting

Schema di troubleshooting 336
Controllo fisico 337
Scambio di componenti di rete 338
Verifica della connettività TCP/IP 340
Analisi lato client 340
Analisi lato server (a livello applicazione) 342
Verifichiamo le conoscenze 343

L6 La sicurezza della rete

Reti sicure 344
Sicurezza nei protocolli TCP/IP 345
Sistemi di controllo e monitoraggio 349
Affidabilità e sicurezza delle strutture 350
Ridondanza di server e servizi 350
Piano di disaster recovery 351
Tecniche di disaster recovery 352
Verifichiamo le conoscenze 354

Esercitazioni di laboratorio

1 Installare Windows 2003 server
2 Installare Active Directory
3 Utility per la verifica della rete
4 Gestire le policies con Active Directory 355
5 Il monitoraggio di Windows Server 366
6 File Server e protezione NTFS 373
7 Politiche di accesso remoto

Puoi scaricare i Lab. 1, 2, 3 e 7 anche da hoepliscuola.it

CLIL 381

AREA digitale

- Architettura del Ministero delle Finanze
- Classificazione dei sistemi Web based
- Impostare i criteri di auditing

Come utilizzare il coupon per scaricare la versione digitale del libro (eBook+) e i contenuti digitali integrativi (risorse online) 386

UNITÀ DI APPRENDIMENTO

1

Il livello delle applicazioni

L1 **Il livello delle applicazioni nei modelli ISO/OSI e TCP**
L2 **Il Web: HTTP e FTP**
L3 **Email, DNS e Telnet**

Esercitazioni di laboratorio

1 Server DNS e HTTP con Packet Tracer; 2 Email server con Packet Tracer; 3 Server FTP con Packet Tracer; 4 HTTP sniffing con Wireshark; 5 DNS e Nslookup; 6 SMTP e POP: sniffing con Wireshark; 7 I proxy server, la navigazione anonima e i cookies ; 8 SMTP in pratica: uso con Telnet

Conoscenze

- Conoscere il concetto di applicazione di rete
- Individuare le tipologie di applicazione di rete
- Comprendere il concetto di porta e di socket
- Conoscere l'architettura peer-to-peer (P2P)
- Comprendere il protocollo Telnet e il suo utilizzo
- Conoscere l'architettura gerarchica del WEB
- Comprendere i meccanismi del protocollo HTTP

Competenze

- Utilizzare i comandi FTP
- Individuare il formato del messaggio HTTP
- Saper individuare le funzioni del client e del server FTP

Abilità

- Utilizzare le principali applicazioni di rete
- Rappresentare le modalità di collegamento FTP

AREA digitale

Esercizi

Soluzioni
Puoi scaricare il file anche da hoepliscuola.it

LEZIONE 1

Il livello delle applicazioni nei modelli ISO/OSI e TCP

In questa lezione impareremo...

- il concetto di applicazione di rete
- le tipologie di applicazione
- le architetture client-server e P2P

Le applicazioni di rete

Nel modello ISO/OSI e TCP il livello delle applicazioni si occupa di implementare le applicazioni di rete che vengono utilizzate dall'utente finale.

> Il livello di applicazione fornisce diversi servizi agli utenti di Internet, la sua flessibilità consente di aggiungere nuovi protocolli, pertanto non è più possibile indicare il numero preciso dei protocolli esistenti, in quanto ne vengono aggiunti costantemente di nuovi.

Il livello applicazione implementa i vari protocolli, tra cui:

- SNMP: Simple Network Management Protocol;
- SMTP: Simple Mail Transfer Protocol;
- POP3: Post Office Protocol;
- FTP: File Transfer Protocol;
- HTTP: HyperText Transfer Protocol;
- DNS: Domain Name System;
- SSH: Secure SHell;
- Telnet.

Nel livello delle applicazioni la comunicazione client-server avviene tramite una connessione logica, dove i livelli applicazioni agiscono come se esistesse un collegamento diretto tra client e server. Un programma (applicazione) che vuole comunicare con un altro programma, deve gestire i primi quattro livelli TCP/IP per aprire la connessione, inviare/ricevere dati e chiudere la connessione. Blocchi di istruzioni di questo tipo vengono chiamate API (Application Programming Interface) o socket.

Host

Un'applicazione di rete è costituita da un insieme di programmi che vengono eseguiti su due o più host contemporaneamente: questi operano interagendo tra loro utilizzando delle risorse comuni, accedendo cioè concorrentemente agli archivi (database), mediante la rete di comunicazione che li connette.

> L'applicazione di rete prende anche il nome di applicazione distribuita dato che non viene eseguita su di un solo elaboratore (concentrata).

ESEMPIO ***Numeri di porte***

Un caso tipico è quello rappresentato da un server sul quale sono disponibili più servizi, tra i quali:

- email: viene inviata usando il protocollo applicativo SMTP, quindi occorre inviare un messaggio opportunamente codificato alla porta TCP 25 del server;
- sito Web: per richiedere una pagina Web si usa il protocollo applicativo HTTP, che invia un opportuno messaggio di richiesta alla porta TCP 80 del server;
- per trasformare un nome di un calcolatore in un indirizzo IP si invia una opportuna richiesta alla porta UTP 53 del server che offre il servizio DNS;

per richiedere il servizio a questo server è quindi necessario specificare l'indirizzo dell'host e il tipo di servizio desiderato.

L'identificazione univoca avviene conoscendo sia l'indirizzo IP che il numero di porta associato al processo in esecuzione su un host: questo meccanismo è già introdotto nelle lezioni precedenti e prende il nome di meccanismo dei ◀ socket ▶.

> ◀ Un socket è formato dalla coppia <indirizzo IP:numero della porta>; si tratta di un identificatore analogo a una porta, cioè a un punto di accesso/uscita: un processo che vuole inviare un messaggio lo fa uscire dalla propria "interfaccia" (socket del mittente) sapendo che un'infrastruttura esterna lo trasporterà attraverso la rete fino alla "interfaccia" del processo di destinazione (socket del destinatario). ▶

Architetture delle applicazioni di rete

Il primo passo che il programmatore deve effettuare per progettare una applicazione di rete è la scelta della architettura dell'applicazione; le principali architetture attualmente utilizzate sono le seguenti:

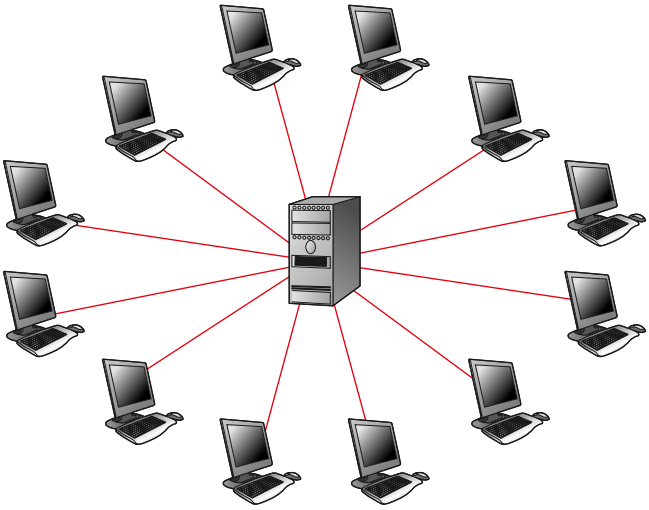
- client-server;
- peer-to-peer (P2P);
- architetture ibride (client-server e P2P).

Architettura client-server

Nella architettura client-server la caratteristica principale è che deve sempre esserci un server attivo che offre un servizio, restando in attesa che uno o più client si connettano a esso per poter rispondere alle richieste che gli vengono effettuate.
Un tipico esempio di questa architettura è il www, dove molteplici server (al limite uno per ogni sito pubblicato) possiedono le pagine (statiche o dinamiche) che saranno inviate ai client che ne fanno richiesta tramite i browser.

Il server deve sempre essere attivo e deve possedere un indirizzo IP fisso dove può essere raggiunto dagli host client: quindi l'indirizzo IP deve essere statico, contrariamente a quello dei client che generalmente è dinamico.
Un client non è in grado di comunicare con gli altri client ma solo con il server: più client possono invece comunicare contemporaneamente con lo stesso server.

Se un server viene consultato contemporaneamente da molti client potrebbe non essere in grado di soddisfare tutte le richieste e potrebbe entrare in stato di congestione: è necessario virtualizzare la risorsa realizzando una server farm: questa non è altro che un server con un unico hostname ma con più indirizzi IP, trasparenti rispetto al client, sui quali vengono dirottate le richieste di connessione (viene utilizzato per esempio da Google, Amazon, Facebook e tutti i siti che hanno una elevata affluenza di visite).



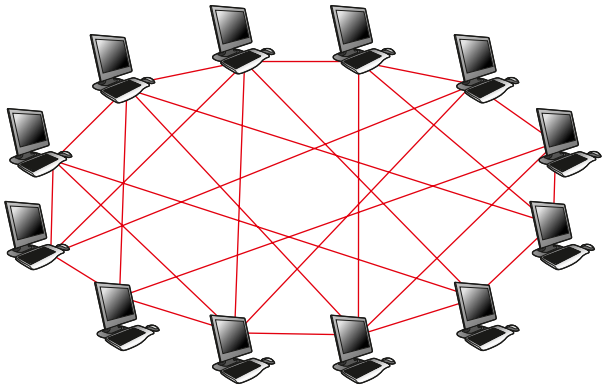
Architettura peer-to-peer (P2P)

Nelle architetture ◀ peer-to-peer ▶ (P2P) abbiamo coppie di host chiamati *peer* (persona di pari grado, coetaneo) che dialogano direttamente tra loro.
Nei sistemi P2P gli host possono essere visti come una comunità che collabora con il binomio dare e ricevere: ogni peer fornisce una risorsa e ottiene in cambio altre risorse.
Gli esempi più noti sono rappresentati dalle reti peer to peer in ambito di condivisione di file, come per esempio eMule, oppure Gnutella.

◀ Peer-to-peer Un sistema Peer to Peer è formato da un insieme di entità autonome (peers), capaci di auto-organizzarsi, che condividono un insieme di risorse distribuite presenti all'interno di una rete. Il sistema utilizza tali risorse per fornire una determinata funzionalità in modo completamente o parzialmente decentralizzato. ▶

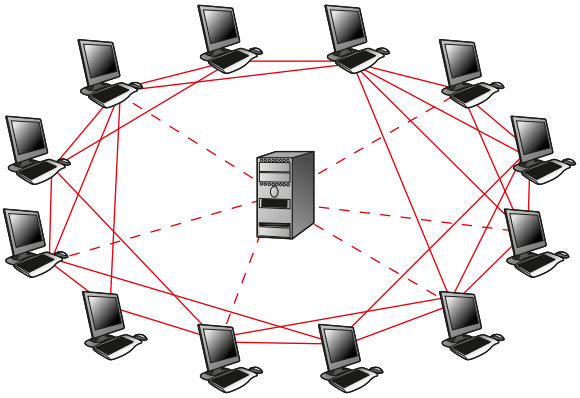
P2P decentralizzato

Nella architettura completamente decentralizzata un peer ha sia funzionalità di client che di server (funzionalità simmetrica = servent), ed è impossibile localizzare una risorsa mediante un indirizzo IP statico: vengono effettuati nuovi meccanismi di indirizzamento, definiti a livello superiore rispetto al livello IP.
Le risorse che i peer condividono sono i dati, la memoria, la banda ecc.: il sistema P2P è capace di adattarsi a un continuo cambiamento dei nodi partecipanti (churn) mantenendo connettività e prestazioni accettabili senza richiedere l'intervento di alcuna entità centralizzata (come un server).



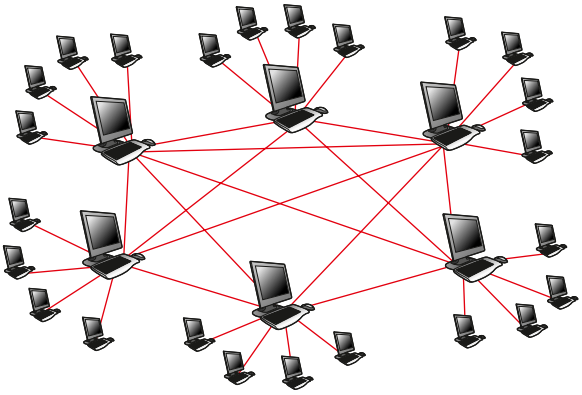
P2P centralizzato

Il P2P centralizzato è un compromesso tra il determinismo del modello client server e la scalabilità del sistema puro: ha un server centrale (directory server) che conserva informazioni sui peer (index, cioè il mapping resorse-peer) e risponde alle richieste su quelle informazioni effettuando quindi la ricerca in modalità centralizzata.
I peer sono responsabili di conservare i dati e le informazioni perché il server centrale non memorizza file, di informare il server del contenuto dei file che intendono condividere e di permettere ai peer che lo richiedono di scaricare le risorse condivise. La sua implementazione più famosa è Napster, dove gli utenti si connettono a un server centrale dove pubblicano i nomi delle risorse che condividono.



P2P ibrido (o parzialmente centralizzato)

Il P2P ibrido è un P2P parzialmente centralizzato dove sono presenti alcuni peer (detti supernodi o super-peer o ultra-peer) determinati dinamicamente (tramite un algoritmo di elezione) che hanno anche la funzione di indicizzazione: gli altri nodi sono anche chiamati leaf peer.



Servizi offerti dallo strato di trasporto alle applicazioni

Le applicazioni richiedono allo strato di trasporto un insieme di servizi specifici oltre ai protocolli necessari per realizzarli, che possono essere standard o realizzati ad hoc.
Tutti i protocolli, sia standard che specifici, hanno in comune una particolarità: trasferire dei messaggi da un punto a un altro della rete. Ogni applicazione deve scegliere tra i protocolli di trasporto quale adottare per realizzare un protocollo applicativo in base ai servizi che sono necessari alle specifiche esigenze della applicazione, che possono essere riassunte in:

- trasferimento dati affidabile;
- ampiezza di banda;
- temporizzazione;
- sicurezza.

Trasferimento dati affidabile

Con trasferimento di dati affidabile intendiamo un servizio che garantisce la consegna completa e corretta dei dati: da una parte sappiamo che alcune applicazioni, come per esempio quelle di audio/video possono tollerare qualche perdita di dati senza compromettere lo scopo dell'applicazione mentre altre, come per esempio il trasferimento di file, richiedono un trasferimento dati affidabile al 100%.
A tale scopo il livello di trasporto mette a disposizione due protocolli:

- UDP User Datagram Protocol: il protocollo di trasporto senza connessione da utilizzarsi quando la perdita di dati è un fatto accettabile;
- TCP Transfer Control Protocol: il protocollo orientato alla connessione da utilizzarsi quando la perdita di dati è un evento inaccettabile, ovvero quando il trasferimento deve essere affidabile.

Ampiezza di banda (bandwidth) o throughput

Alcune applicazioni, come per esempio quelle multimediali, per poter "funzionare" hanno bisogno di avere una garanzia sulla larghezza di banda minima disponibile, cioè possono richiedere un throughput garantito di R bit/s: si pensi alla trasmissione di un evento in diretta in una Web-TV.
Altre applicazioni, invece, non hanno questo bisogno come prioritario, ma utilizzano in modo elastico l'ampiezza di banda che si rende disponibile: tipici esempi sono la posta elettronica o i sistemi FTP.

> Sappiamo che Internet ha una natura eterogenea e quindi i protocolli di trasporto non sono in grado di garantire la presenza di una certa quantità di banda per tutta la durata necessaria per trasmettere un messaggio ma, come vedremo, mette a disposizione la possibilità di implementare un protocollo applicativo flessibile che realizza un circuito virtuale che fallisce o se adatta se la banda è insufficiente.

Temporizzazione

Alcune applicazioni, come la telefonia VoIP, i giochi interattivi, gli ambienti virtuali, per essere "realistiche" ammettono solo piccoli ritardi per essere efficaci: lo strato di trasporto non è in grado di garantire i tempi di risposta perché le temporizzazioni presenti assicurano un certo ritardo end-to-end tra le applicazioni.
Il protocollo TCP garantisce la consegna del pacchetto, ma non il tempo che ci impiega e neppure il protocollo UDP, nonostante sia più veloce del TCP, è temporalmente affidabile.

La soluzione, come vedremo, è quella di utilizzare un protocollo di trasporto in tempo reale, come RTP (Real Time Protocol), che è in grado di studiare i ritardi di rete e calibrare gli apparati e i collegamenti per garantire di restare nei limiti di tempo prefissati, scegliendo alternativamente quando utilizzare UDP e quando TCP.

Sicurezza

Una applicazione può richiedere allo strato di trasporto anche la cifratura di tutti i dati trasmessi in modo tale che anche se questi venissero intercettati da malintenzionati non si perda la riservatezza.
È quindi possibile che vengano richiesti dei servizi di sicurezza da applicare per garantire l'integrità dei dati e l'autenticazione end-to-end.

La tabella seguente riporta i requisiti richiesti al servizio di trasporto da parte di alcune applicazioni comuni.

Applicazioni	Tolleranza alla perdita dei dati	Ampiezza di banda	Sensibilità dal tempo
Trasferimento file	No	Variabile	No
Posta elettronica	No	Variabile	No
Documenti Web	No	Variabile	No
Audio/Video in tempo reale	Sì	Audio: da 5 Kbps a 1 Mbps Video: da 10 Kbps a 5 Mbps	Sì, centinaia di ms
Audio/Video memorizzate	Sì		Sì, poche secondi
Giochi interattivi	Sì	Fino a pochi Kbps	Sì, centinaia di ms
Messaggistica istantanea	No	Variabile	Sì e no

Verifichiamo le conoscenze

1. Risposta multipla

1 Quale tra i seguenti non è un protocollo applicativo?

a. HTTP
b. POP3
c. DNS
d. SMNP
e. SMTP
f. FTP

2 Quale tra le seguenti non è un'applicazione di rete?

a. Posta elettronica
b. Condivisione di file P2P
c. Scheduler dei processi
d. Telefonia via Internet
e. Videoconferenza in tempo reale
f. TV in streaming
g. Telnet

3 Cosa significa SMTP?

a. Simple Message Transfer Protocol
b. System Mail Transfer Protocol
c. Simple Mail Transfer Protocol
d. System Message Transfer Protocol

4 Qual è il significato di API?

a. Application Protocol Internet
b. Application Protocol Interface
c. Application Programming Interface
d. Application Programming Internet

5 Quali tra le seguenti non sono architetture di un'applicazione di rete?

a. Client-server
b. B2B
c. B2C
d. P2P

6 Quale tra i seguenti servizi offerti non è garantito dallo strato di trasporto alle applicazioni?

a. Trasferimento dati affidabile
b. Ampiezza di banda
c. Velocità di comunicazione
d. Temporizzazione
e. Sicurezza

2. Associazione

1 Effettua il corretto accoppiamento:

1 ..... messaggio	a) datagramma
2 ..... trasporto	b) frame
3 ..... rete	c) segmento
4 ..... collegamento	d) applicazione

3. Vero o falso

1 Il protocollo HTTP è a livello di trasporto. V F

2 Il protocollo TCP è a livello di applicazione. V F

3 L'applicazione di rete prende anche il nome di applicazione distribuita. V F

4 L'applicazione di rete prende anche il nome di applicazione multiutente. V F

5 Sullo stesso host possono essere in esecuzione molti processi. V F

6 Sullo stesso host può essere in esecuzione una sola applicazione. V F

7 Un protocollo è una parte integrante di una applicazione ed è sviluppato all'interno di essa. V F

8 In una architettura client-server gli indirizzi IP devono essere statici. V F

9 Il termine servent è ottenuto dalla contrazione server-client. V F

10 Nel P2P decentralizzato i servent hanno indirizzo IP statico. V F

Verifichiamo le competenze

Completamento

1 Completa le seguenti tabelle.

Applicazione	Tolleranza alla perdita dei dati	Ampiezza di banda	Sensibilità dal tempo
Trasferimento file			
Posta elettronica			
Documenti Web			
Audio/video in tempo reale			
Audio/video memorizzate			
Giochi interattivi			
Messaggistica istantanea			

Caratteristiche del protocollo	UDP	TCP
Orientato alla connessione		
Trasferimento affidabile		
Garantisce trasporto senza errore		
Effettua il controllo di flusso		
Esegue anche il controllo della congestione		
Dà garanzie di banda minima		
Dà garanzie di ritardo minimo		

Applicazione	Protocollo applicativo	Protocollo di trasporto sottostante
Posta elettronica		
Accesso a terminali remoti		
Web		
Trasferimento file		
Multimedia streaming		
Telefonia Internet		

LEZIONE 2

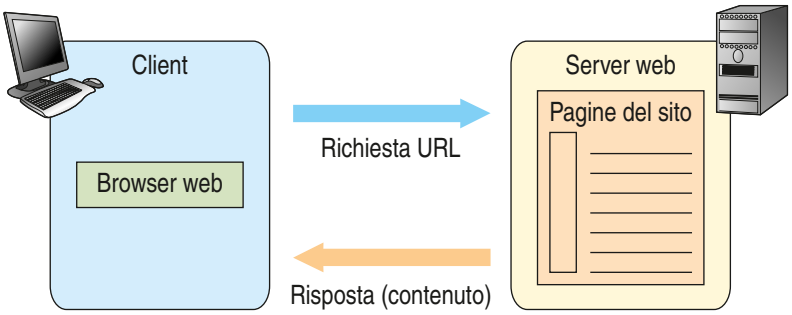
Il Web: HTTP e FTP

In questa lezione impareremo...

- l'architettura del Web
- il protocollo HTTP
- il protocollo FTP

Il World Wide Web

WWW (World Wide Web) significa "ragnatela intorno al mondo" ed è un insieme di pagine multimediali, documenti testuali, audio e video, collegati tra loro, entro i quali ci si può spostare con diverse modalità. In sostanza, è l'insieme delle pagine ipermediali di Internet, cioè è un ipertesto multimediale distribuito.
Lo schema che definisce il funzionamento del www è presentato nella figura che segue.



Una pagina, detta home-page, viene inviata come risposta, all'atto del collegamento, a un indirizzo specifico e per essere visualizzata sull'host che ne ha fatto la richiesta è necessario l'uso di un ◀ browser ▶, un programma client per la visualizzazione dei documenti e per la navigazione in rete.

◀ Browser Significa letteralmente "sfogliatore" e non è altro che un programma in grado di "locare" una pagina in Internet e di interpretarne attraverso un parser interno le righe di codice sorgente scritte in HTML, fornendo all'utente una linea di comando dove poter digitare gli indirizzi IP. ▶

Il codice sorgente delle pagine Web che viene interpretato è scritto in un linguaggio di "contrassegno" quale HTML, che nelle ultime versioni è anche in grado di mandare in esecuzione pseudoeseguibili scritti in Java (Applet) o di interpretare programmi incapsulati internamente, detti script, quali per esempio VBscript, Jscript o il più conosciuto JavaScript. I browser più diffusi sono certamente Microsoft Edge, Internet Explorer, Chrome, Opera, Mozilla e altri meno noti.

Il client fornisce a un server le richieste per un determinato oggetto. Il server risponde con i dati richiesti inviandoli in formati standard integrandoli col codice HTML. Questo è un modello di carattere generale, tuttavia sarà importante ricordare questo schema di comunicazione quando verranno discussi i linguaggi di scripting lato server (PHP e ASP).

L'architettura del Web

All'interno della rete Internet ciascuna risorsa è identificata in modo univoco mediante un indirizzo URI (Universal Resource Identifier). L'URI non è altro che un indirizzo univoco di una particolare risorsa nella rete, rappresenta la risorsa che si vuole raggiungere. Per capire il funzionamento del Web vediamo un piccolo esempio che aiuta a comprendere cosa accade quando un utente si vuole collegare a un certo indirizzo URI, in questo caso al sito http://www.istruzione.it.
Si scrive nell'apposita barra del browser l'indirizzo http://www.istruzione.it.

- Il browser recupera le informazioni secondo i meccanismi previsti per le risorse identificate con lo schema URI-HTTP;
- il server che contiene le pagine Web del sito www.istruzione.it risponde alla richiesta inviando le informazioni che si vogliono ottenere;
- il browser interpreta la risposta, identificando il tipo di documento che viene trasmesso (content-type) e a sua volta invia altre richieste per recuperare le informazioni collegate, quali per esempio le immagini relative alle notizie dell'ultim'ora;
- il browser mostra le informazioni ricevute, che includono a loro volta collegamenti ipertestuali.

L'URI comprende tutto quanto è necessario per l'indirizzamento e la localizzazione dei file. Esso infatti include la localizzazione del protocollo, l'indirizzo Internet e il nome del file, ed eventualmente la localizzazione interna a quel particolare documento. Questo argomento verrà approfondito più avanti.

URL (Uniform Resource Locator)

Generalmente si sente parlare di URL (Uniform Resource Locator) e non di URI, ma la differenza tra i due riferimenti a indirizzi Internet sta nel fatto che l'URL è un particolare tipo di URI e un URI può identificare oggetti anche non correlati ai protocolli Internet esistenti (si pensi per esempio al caso di about:netscape).

Ogni documento Internet è individuato da un indirizzo URL che lo identifica in modo univoco, che è formato da:

- protocollo per la connessione (HTTP per pagine Web);
- nome simbolico (o indirizzo IP) del server;
- pathname del file sul server.

In pratica un URI è un URL più generale che non fa riferimento a un preciso schema di denominazione.

ESEMPIO

http://www.lorusso.it/Sistemi/Volume3/index.html

È anche possibile inoltre indicare la porta a cui connettersi e passare dei parametri alla risorsa richiesta:

http://www.lorusso.it:8083/Sistemi/Volume3/page.php?param=value

Vedremo che l'associazione tra il nome dell'host e il suo indirizzo IP viene effettuata da un'apposita applicazione, DNS (Domain Name System).
L'architettura di funzionamento del Web può essere espressa mediante tre termini assai importanti che ne descrivono le caratteristiche: identificazione, interazione e formato.

L'identificazione

Mediante un indirizzo (URI o URL) le risorse presenti nella rete possono essere univocamente identificate.

L'interazione

I browser comunicano mediante protocolli standard che permettono l'interazione tramite l'interscambio di informazioni strutturate secondo una sintassi e una semantica precise. Infatti quando si clicca su un link o ci si collega a un indirizzo Web, si dice al browser di ricercare una risorsa identificata da quell'indirizzo.

Il formato

Nel protocollo di comunicazione sono previste informazioni aggiuntive, chiamate meta-informazioni che permettono di identificare il tipo di documento da trasferire o da interpretare.

Zoom su...

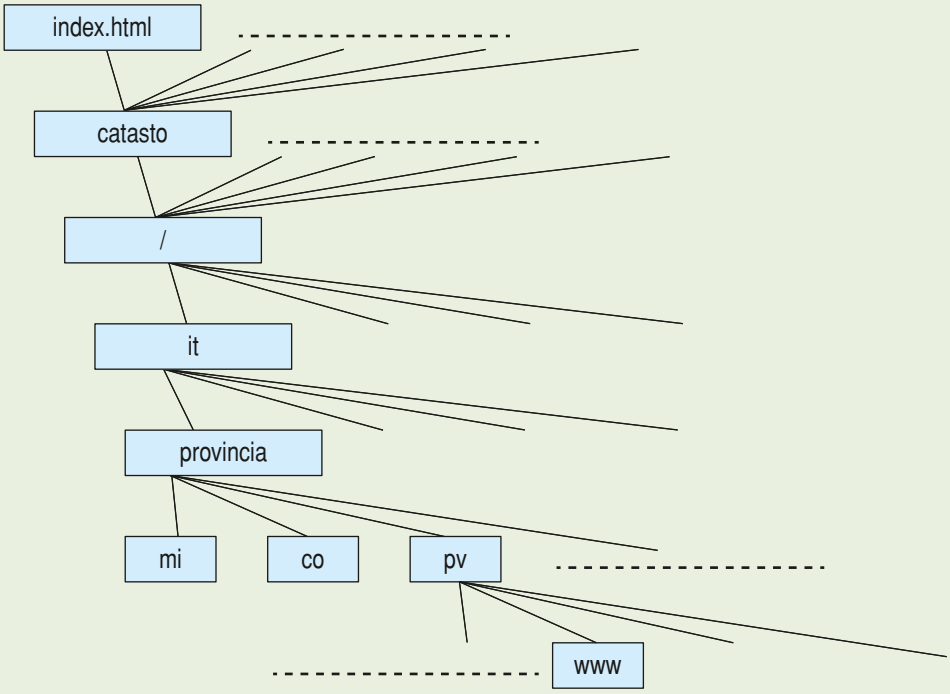
LA SINTASSI URL

La sintassi prevede che venga indicato il protocollo per primo, quindi le informazioni del dominio, poi l'eventuale country-code, quindi le eventuali directory e infine il file che contiene i dati.

protocollo usato: sottodominio"n".sottodominio"n–1"…dominio/directory/file

Il dominio può possedere anche dei sottodomini, per esempio nell'indirizzo
http://www.mi.provincia.it
mi è un sottodominio di provincia, oppure nell'url http://www.mi.provincia.it/cataloghi/anni/2012/miocatalogo.htm,
cataloghi è la directory del server di dominio che contiene la directory anni che a sua volta contiene la directory 2012 che a sua volta contiene il file. www invece indica il Web server, infatti può essere sostituito con il nome della macchina che lo ospita, per esempio l'URL "http://www.lombardia.regione.it" rispetto a "http://italia.lombardia.regione.it", presenta "italia" che non è altro che la macchina che fisicamente ospita il Web server.

I domini vengono appunto suddivisi gerarchicamente: più nomi di macchine fanno riferimento a un dominio, più nomi di domini fanno riferimento a un dominio di alto livello. Per esempio l'URL "http://www.pv.provincia.it/catasto/index.html" può essere schematizzato come segue:



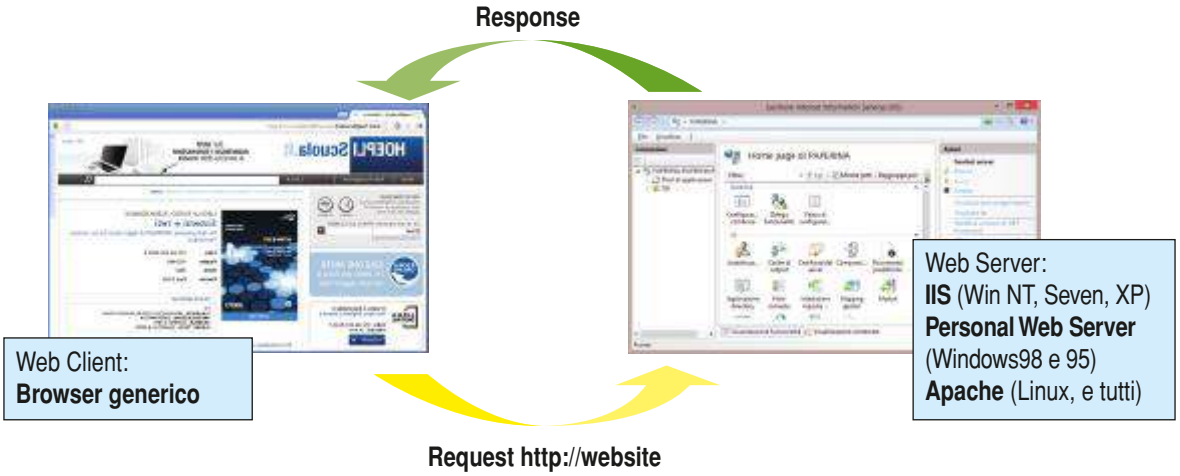
Ma che cos'è un dominio di alto livello? Si tratta di un dominio che identifica la tipologia e la topologia di un sito.
Vediamo una tabella che ne descrive alcuni:

.com	per organizzazioni a carattere commerciale	**.gov**	per enti governativi americani
.edu	per organizzazioni di ricerca americane	**.uni**	solo per università americane
.net	per organizzazioni che forniscono servizi di rete	**.org**	per società o organizzazioni non commerciali
.it	Italia	**.fr**	Francia
.de	Germania	**.uk**	Gran Bretagna
.mn	Mongolia	**.my**	Malesia
.hk	Hong Kong	**.tr**	Turchia
.cu	Cuba	**.ir**	Iran
.cg	Congo	**.ch**	Svizzera
.biz	Business	**.tv**	Televisioni

Da come si può vedere in questa tabella, che ne riassume solo alcuni, i suffissi di dominio sono divisi in country-code e in society-code, i primi nazionali e i secondi invece legati a enti, aziende o associazioni. Tuttavia uno dei problemi che ultimamente è venuto alla ribalta è proprio legato a come questi suffissi non siano più sufficienti e vi sia la necessità di nuove adozioni.
Anche per gli indirizzi di posta elettronica deve essere indicato un URL, che è composto dai seguenti componenti: **mailto:username@dominio**
Per esempio nell'URL "mailto:zio.pino@co.provincia.it" il dominio è composto da un host principale (provincia.it) e da un sottohost denominato co.

Il protocollo HyperText Transfer Protocol (HTTP)

Il World Wide Web per il trasferimento di dati ipertestuali si basa sul protocollo applicativo HyperText Transfer Protocol (HTTP) che, come tutti i servizi di rete, utilizza l'architettura client-server. Il protocollo HTTP è definito in RFC 1945 (versione 1.0) e RFC 2616 (versione 1.1), inoltre è basato sullo scambio di messaggi tra client e server. Come si vede nella figura, abbiamo a sinistra il browser (client) e a destra il server (rappresentato in questo caso da un IIS – Internet Information server – che non è altro che un server Web utilizzato in tutti i sistemi operativi della Microsoft):



La comunicazione tra client e server avviene secondo il protocollo TCP/IP usando gli indirizzi IP dei computer che ospitano client e server.
I messaggi con il protocollo HTTP possono essere separati nelle due categorie request e response, cioè richiesta e risposta, e sono un insieme di righe di caratteri ASCII terminate da CR+LF. I due messaggi hanno lo stesso formato, secondo lo standard RFC822, e sono entrambi definiti dal protocollo.
Il meccanismo che sta alla base della comunicazione attraverso il protocollo HTTP è il seguente:

- si apre una connessione TCP tra client e server;
- il browser richiede una risorsa al server HTTP (Web server);
- il server risponde (se possibile, fornendo la risorsa richiesta);
- si chiude la connessione (da HTTP1.1 non si chiude automaticamente ogni volta la sessione, ma rimane aperta per dare maggiori possibilità di trasmissione dati).

Vediamo adesso come si apre la connessione tra client e Web server in una tipica "conversazione" tramite protocollo HTTP, per esempio per la seguente richiesta:

http://alinet.miur.unibc.it/sistemi/itisVol2/RetiLaB/index.html

1. Il browser del client analizza l'URL e ne estrae il dominio;
2. il client HTTP inizia una connessione TCP verso il Web server alinet.miur.unibc.it sulla cui porta 80 il server HTTP è in ascolto;
3. il client HTTP invia una richiesta (GET), al server attraverso il socket, associata alla connessione TCP stabilita al punto 1; nella richiesta specifica il file /sistemi/itisVol2/RetiLaB/index.html;
4. il server riceve la richiesta, incapsula l'oggetto specificato nella risposta HTTP e invia il messaggio al client attraverso il socket;
5. il server HTTP invia quindi al TCP la richiesta di chiusura della connessione, che avverrà solo dopo che il messaggio di risposta è stato riscontrato dal client;
6. la connessione TCP si conclude; il messaggio indica che l'oggetto è un file HTML; il client lo estrae e trova i riferimenti agli oggetti referenziati (immagini, fogli di stile, oggetti Javascript ecc.);
7. i passi precedenti vengono ripetuti per ciascuno degli oggetti referenziati (eventualmente aprendo più connessioni in parallelo).

La connessione creata da HTTP 1.0 è di tipo non permanente: si limita alla trasmissione di una singola pagina HTML.
La modalità di default per HTTP 1.1 è invece di tipo permanente: il server non chiede la chiusura della connessione TCP se non dopo che è scaduto un time-out durante il quale la connessione non è utilizzata.

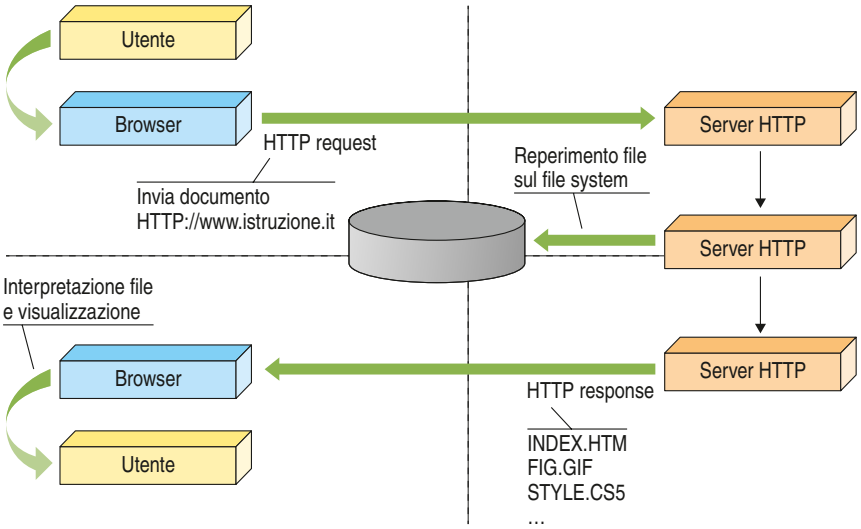
Il formato del messaggio HTTP

Il formato dei messaggi HTTP è composto da una start-line (riga di richiesta/risposta), una HEADER (intestazione HTTP) e da un BODY (corpo HTTP, che può anche essere omesso). Vediamoli più in dettaglio.

La prima riga della richiesta contiene 3 elementi, un comando chiamato metodo (GET e POST sono i più usati, poi ne vedremo le differenze, ma esistono anche HEAD, PUT, DELETE, TRACE, CONNECT, OPTIONS, per maggiori chiarimenti guardare il sito www.rfc.net), il secondo è il percorso del server della richiesta del client e poi la versione del protocollo HTTP usata (di solito 1.1).
Nella intestazione (HEADER) compaiono invece i dati che riguardano il tipo di documento che il client riceve dal server, il tipo di browser che ha richiesto la pagina, la data e alcune informazioni generali sulla configurazione del sistema richiedente. Il corpo (BODY) del messaggio di richiesta da parte del client, può essere omesso, verrà usato invece dal server per rispondere con la pagina HTML vera e propria. Conterrà i dati di un eventuale form inviato al server SOLO se è stato usato il metodo POST. Nella riga risposta del server invece compaiono solo 2 informazioni: il numero delle versioni dell'HTTP e un codice di risposta tra i seguenti.

CLASSE	DESCRIZIONE
100-199	Risposta in fase di elaborazione
200-299	Successo
300-399	La richiesta non è stata evasa in quanto le informazioni richieste sono state spostate
400-499	La richiesta è incompleta, errata o impossibile (è tipico l'errore 404: server non trovato)
500-599	Errore nel server, con richiesta però valida

Nell'intestazione della risposta compaiono 3 dati: il primo di tipo generale (per esempio data e ora di risposta), il secondo è l'entità (per esempio data e ora di ultima modifica dei dati richiesti) e il terzo è la richiesta (informazioni sul server e su come gestisce la risposta, se i dati sono text o HTML ecc.). Il corpo della risposta contiene la pagina HTML vera e propria. Vediamo lo schema logico di quanto appena detto:



ESEMPIO

Vediamo adesso tre esempi di richiesta/risposta.

1 Esempio di richiesta.

```
GET /sistemi/itisVol2/RetiLaB/index.html HTTP/1.1   */* metodo, file, versione
Accept:                                             */* contenuto accettato
Accept-Language: en-us                              */* preferenza linguistica
If-Modified-Since: Wed, 16 Jan 2012 12:37:40 GMT    */* ultima versione nella cache
User-agent:Mozilla/4.0                              */* tipo di browser
Host: alinet.miur.unibc.it                          */* host
Connection: Keep-Alive                              */* connessione permanente
```

2 Esempio di risposta positiva.

```
HTTP/1.1 200 OK
Date: Wed, 22 Mar 2013 17:37:44 GMT
Content-Length: 12692
Content-Type: text/html
Server: Apache/2.0.40 (Red Hat Linux)
Last-Modified: Mon, 01 Mar 2013 18:02:44 GMT
<html>
…
qui c'è il testo HTML della pagina richiesta (12692 byte)
…
</html>
```

3 Esempio di risposta negativa (il file richiesto non esiste).

```
HTTP/1.1 404 Not Found
Date: Wed, 02 Mar 2013 17:38:37 GMT
Content-Length: 1067
Content-Type: text/html
Server: Apache/2.0.40 (Red Hat Linux)
<html>
…
Object not found
…
Error 404
…
</html>
```

Definizioni dei metodi

HTTP mette a disposizione del client un insieme di metodi per inviare le richieste al server: questi metodi sono a tutti gli effetti dei comandi che il client invia al server. Vediamoli in sintesi.

OPTION

Il metodo OPTION rappresenta una richiesta di informazioni inerenti alle opzioni di comunicazione disponibili sul canale definito dalla Request-URI.

GET
Il metodo GET richiede una risorsa (informazioni, file, documenti, pagine HTML) al server localizzato con una Request-URI.

HEAD
Il metodo HEAD è identico al GET eccetto per il fatto che il server non deve restituire il corpo del messaggio, ma solamente l'header. Il metodo viene usato spesso per testare la accessibilità e le recenti modifiche di link ipertestuali.

POST
Con il metodo POST il client può spedire al server informazioni organizzate con una serie di coppie *nome=valore* che corrispondono all'input del programma indicato nella request-URI.

PUT
Il metodo PUT serve per inviare file al server (upload di file da parte del client): se il file esiste in corrispondenza all'URI specificato, questo verrà considerato come un aggiornamento della versione preesistente.

DELETE
Il metodo DELETE richiede che il server ricevente cancelli il file all'indirizzo specificato dal Request-URI. Il client non ha nessuna garanzia che l'operazione abbia esito positivo in quanto è necessario che esso possieda i diritti per eseguire questa operazione.

TRACE
Il metodo TRACE richiama un loopback remoto a livello dell'applicazione del messaggio richiesto: si tratta di un "ping" che verifica quali dati il server Web riceve dal client.

CONNECT
Questo metodo viene usato per instaurare una semplice connessione con un proxy server.

I cookies

Il protocollo HTTP non permette che il server contattato "riconosca" un utente che si è già collegato, dato che ogni pagina inviata richiede una connessione TCP indipendente; inoltre dato che il protocollo HTTP è state-less e quindi le richieste dei client non lasciano alcuno stato nel server, è necessario memorizzare le informazioni della sessione sull'applicazione Web direttamente nel Web Browser del visitatore. I cookies sono una parte fondamentale del protocollo HTTP che permettono di riconoscere un utente. Un cookie è un file che viene memorizzato nel computer del client dal sito Web che viene visitato, contenente informazioni sulle pagine visitate dall'utente: quando l'utente si ricollega, il contenuto di tale file viene mandato al server, che lo analizza e ne estrae informazioni che ha precedentemente memorizzato in modo da presentare le informazioni personalizzate in base alle esigenze del visitatore (per esempio la lingua preferita, i dati di login per non richiedere ripetutamente le credenziali di accesso ad aree riservate, la personalizzazione della visita con la visualizzazione delle preferenze già definite dall'utente in accessi precedenti ecc.). In alcuni browser ogni cookie corrisponde a un piccolo file mentre per esempio in Firefox tutti i cookie sono memorizzati in un singolo file.

Per poter scrivere i cookies sul computer dell'utente il server ha necessariamente bisogno della autorizzazione del client che deve abilitare tra le opzioni di configurazione del suo browser e di protezione del suo computer la possibilità di memorizzare i cookies da parte di altri host.

HTTPS: Secure HyperText Transfer Protocol (cenni)

Il normale traffico effettuato attraverso il browser col protocollo HTTP non pone in relazione i dati tra le sessioni precedenti e le successive e quindi rende di fatto "indipendente" ogni coppia di operazioni request-responce.

◀ I packet sniffer sono programmi di utilità che consentono di catturare i pacchetti prelevandoli dal traffico della rete, utili per risolvere eventuali problemi verificatisi nella rete o soltanto per controllare il regime del traffico. ▶

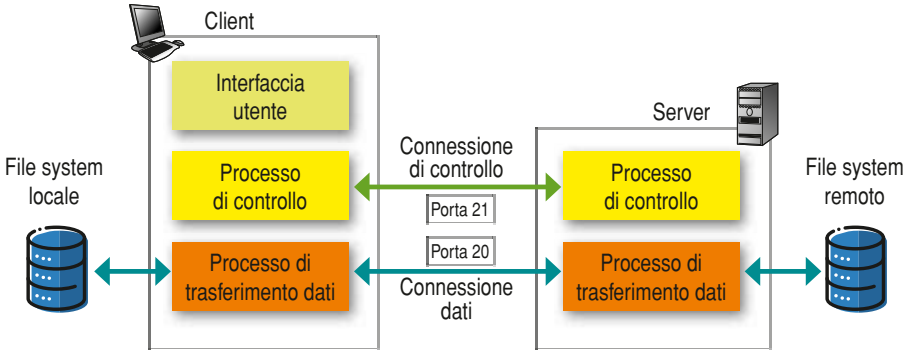
Supponiamo di voler effettuare un acquisto su un sito Web e di dover quindi inviare informazioni riservate e personali: prima di arrivare a destinazione, i nostri dati, il numero della carta di credito e qualsiasi altra informazione ci riguardi, attraversano un numero imprecisato di nodi e sono visibili chiaramente con l'utilizzo di un semplice programma di ◀ packet sniffer ▶.

La soluzione di questo problema è stata realizzata con la definizione del protocollo HTTPS descritto nella RFC 2965, che incapsula HTTP in una connessione cifrata con il Web Server di destinazione in modo da rendere più complesso, o per lo meno più macchinoso, un attacco da parte di malintenzionati.

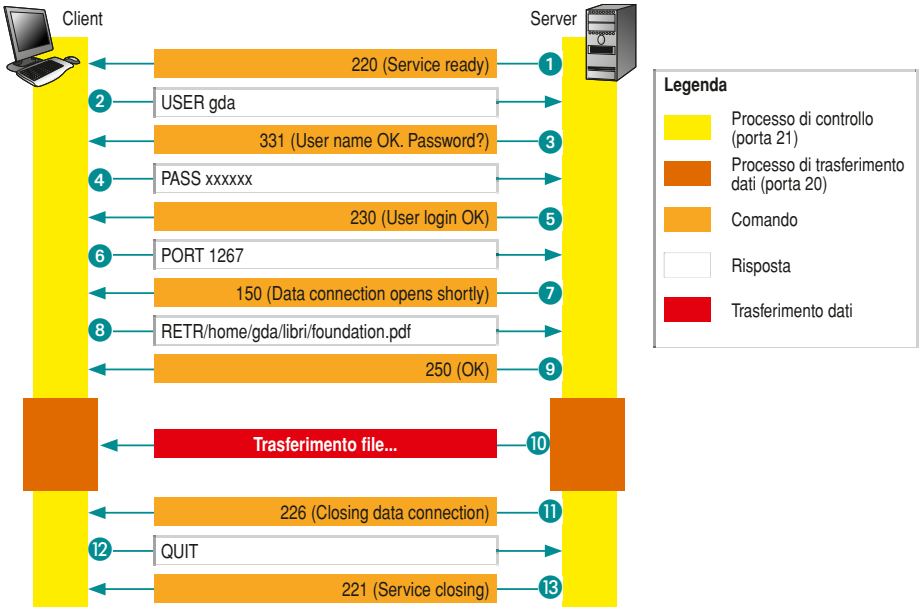
Il protocollo FTP

Il protocollo utilizzato a livello applicativo per trasferire i file è il File Transfer Protocol, comunemente chiamato FTP, che si basa su TCP ed è stato definito nel 1984 nel RFC 959.
A differenza di altri protocolli, FTP per trasportare un file utilizza due canali TCP separati che agiscono in parallelo, cioè una connessione di controllo e una connessione dati:

- la prima connessione è usata per spedire le informazioni di controllo tra client e server, come l'identificazione dell'utente, password, comandi per la variazione della directory remota ecc.): viene normalmente chiamata control connection o command channel;
- la seconda connessione è quella effettivamente utilizzata per il trasferimento dei file: viene normalmente chiamata data connection o data channel.



Il protocollo FTP si riferisce a un modello di tipo client-server dove la macchina host destinata a svolgere la funzione di server ha in esecuzione uno specifico programma che può essere fornito direttamente col sistema operativo oppure istallato in un secondo tempo.
Per poter realizzare la connessione FTP entrambe le macchine devono avere istallato un software FTP, rispettivamente un FTP client e un FTP server.



FTP server

Esistono in distribuzione parecchi software FTP validi, sia distribuiti gratuitamente con licenza open source, sia a pagamento, come per esempio Filezilla Server.

Il software FTP server mette a disposizione dei client molteplici opzioni per interagire con l'insieme dei file condivisi nel suo file system, tra cui:
- download/upload di file;
- recupero (resume) di trasferimenti interrotti;
- rimozione e rinomina di file;
- creazione di directory;
- navigazione tra directory.

L'accesso al FTP server viene effettuato mediante un sistema di autenticazione e in base alle credenziali possono essere assegnati determinati privilegi agli utenti registrati per poter operare sul file system: spesso è anche possibile effettuare l'autenticazione "anonima", cioè quella che effettua un client che non specifica alcuna password di accesso: in questo caso, generalmente, gli viene concesso come privilegio quello di poter effettuare la "sola lettura".

FTP client

Anche la connessione da parte del client avviene mediante un apposito software, generalmente gratuito, capace di connettersi a un server e di caricare file dal proprio computer al server, quindi caricare il contenuto a un indirizzo Web, o downloadare file da un server a un particolare indirizzo IP.
Generalmente un FTP client è un programma costituito da due componenti:
- parte di comunicazione: implementa il protocollo FTP;
- interfaccia utente: generalmente di tipo grafico agevola lo svolgimento delle funzioni offerte dal prodotto.

I diversi programmi si differenziano dalle opzioni offerte all'utente, che vanno da quella di permettere upload multipli, alla scelta della velocità, al transfer da server a server, ai componenti grafici dello stato e dell'avanzamento dei trasferimenti, all'interfaccia grafica accattivante, alla possibilità di interrompere il download quando si vuole e riprenderlo senza file corrotti.
Le funzioni comuni a tutti i programmi sono le seguenti:
- connessione al server remoto;
- trasferimento di un file dal server al client (get);
- trasferimento di un file dal client al server (put);
- lettura dei file presenti nella directory corrente sul server (dir);
- cambiamento di directory corrente sul server (cd);
- disconnessione (bye).

Uno del principali client FTP è Filezilla.

FTPS

Sempre in termini di sicurezza, è doveroso ricordare che il protocollo FTP non prevede alcuna cifratura per i dati scambiati tra client e server e tra questi vengono scambiati nomi utenti, password, comandi, codici di risposta e file trasferiti che possono essere agevolmente "sniffati" da malintenzionati.
Per ovviare a questo problema è stata definita una nuova specifica, la RFC 4217, che aggiunge al protocollo FTP originale un layer di cifratura SSL più una nuova serie di comandi e codici di risposta: tale protocollo prende il nome di FTPS.

> Tutti i trasferimenti FTPS sono cifrati e l'algoritmo di cifratura è negoziato con il server: se viene impostato, la finestra del trasferimento mostrerà il simbolo di un "lucchetto" a indicare il trasferimento sicuro.

Verifichiamo le conoscenze

1. Risposta multipla

1 Indica la differenza tra router, ISP e host.

a. Router instrada i pacchetti, mentre l'ISP distribuisce le connessioni ai Web client e host è sinonimo di computer che ospita fisicamente un sito
b. Router distribuisce le connessioni ai Web client, mentre l'ISP instrada i pacchetti e host è sinonimo di computer che ospita fisicamente un sito
c. Router è sinonimo di computer che ospita fisicamente un sito, mentre l'ISP distribuisce le connessioni ai Web client e host è il computer che instrada i pacchetti
d. Router instrada i pacchetti, mentre l'ISP distribuisce le connessioni di posta elettronica e host è sinonimo di computer che ospita fisicamente un sito

2 L'URL ftp:miosito.com indica:

a. che il protocollo usato è ipermediale e che il sito si trova a Roma
b. che il protocollo usato è ipermediale e che il sito si trova in Italia
c. che il protocollo usato è di trasferimento file e che il sito si trova a Roma
d. che il protocollo usato è di trasferimento file e che il sito è di tipo commerciale

3 Indica il protocollo dal livello fisico più basso tra i seguenti protocolli:

a. TCP b. IP c. FTP d. TELNET

4 Il protocollo HTTP permette:

a. il trasferimento di file
b. di avere una connessione in tempo reale tra due host remoti
c. il trasferimento di dati ipertestuali
d. il trasferimento di file per la posta elettronica

5 Dove è definito il formato dei messaggi HTTP?

a. UNI b. RFC c. ISO d. OSI

6 Il software FTP server mette a disposizione le seguenti opzioni (indica quella errata):

a. download di file
b. upload di file
c. cifratura dei file
d. recupero di trasferimenti interrotti
e. rimozione e rinomina di file
f. creazione di directory
g. navigazione tra directory

7 Il trasferimento di un file dal server al client può essere fatto con:

a. collegamento normale
b. collegamento diretto
c. collegamento attivo
d. collegamento passivo

2. Ordinamento

1 Metti in ordine logico le operazioni seguenti che avvengono durante una comunicazione client-server secondo il protocollo HTTP.

a) ..... si apre una connessione TCP tra client e server
b) ..... si chiude la connessione
c) ..... il server risponde (se possibile, fornendo la risorsa richiesta)
d) ..... il browser richiede una risorsa al server HTTP (Web server)

2 Metti in ordine logico le seguenti operazioni che avvengono a livello client in una conversazione HTTP.

a) ..... la pagina multimediale è caricata sul browser
b) ..... il browser apre una connessione TCP con il Web server (porta 80)
c) ..... il browser analizza l'URL e ne estrae il dominio
d) ..... il browser consulta il DNS per ottenere l'indirizzo IP corrispondente al dominio
e) ..... una volta stabilita la connessione, il browser e il server usano HTTP per comunicare

LEZIONE 3

Email, DNS e Telnet

In questa lezione impareremo...

- il funzionamento della posta elettronica
- le funzioni del DNS
- il protocollo Telnet

Il servizio email

Il successo di Internet è stato anche determinato dal servizio di posta elettronica o più correttamente email (dall'inglese «electronic mail»), che senza dubbio è l'applicazione più utilizzata in rete, sia da privati, per comunicare con amici al posto del tradizionale documento cartaceo, sia da aziende, per le normali transazioni commerciali e per inviare ai possibili clienti quantità "sproporzionate" di messaggi commerciali (◀ spam ▶) dato che il loro costo è praticamente nullo.

◀ Spam La parola spam (*spiced ham*) era usata negli Stati Uniti d'America per indicare un tipo particolare di carne in scatola, fornita all'esercito americano, di pessima fama. Nel gergo di Internet spam indica l'insieme dei messaggi email indesiderati, soprattutto di tipo pubblicitario. ▶

Gli indirizzi di posta elettronica, in Internet, hanno la forma:
nomeutente@dominio
dove

- nomeutente è la stringa che identifica l'interlocutore (mittente o destinatario) che è univoca per dominio: è un nome scelto dall'utente o dall'amministratore del server, che identifica in maniera univoca un utente;
- dominio è rappresentato dal nome del provider e dalla nazionalità oppure da un indirizzo IP.

Il carattere "chiocciola" (@, in inglese "at") è usato nella posta elettronica per indicare "presso". Nasce intorno al VI-VII secolo, più tardi viene usato in Inghilterra per scopi commerciali e stava a indicare "al prezzo di". Per esempio, in fattura si scriveva: *five barrels @ 200 pence each*.
Quando nel 1972 venne creata la rete ARPANET (antenata di Internet) venne usata per la prima volta la chiocciola per separare il nome utente dal server negli indirizzi email.

Dobbiamo sottolineare come l'indirizzo di posta elettronica non sia associato a una persona, ma a una casella postale elettronica; ogni utente può possedere diverse caselle come è anche possibile associare nomi utente diversi (alias) alla stessa casella di posta.
È inoltre doveroso fare una precisazione differenziando la posta elettronica in funzione delle modalità di accesso a essa, che può essere di due tipi:

- POP mail;
- Web mail.

La POP mail permette di leggere e inviare i messaggi di posta elettronica dal computer nel quale è installato il programma di posta elettronica preferito, genericamente chiamato ◀ client di posta ▶. Ne esistono molti in commercio tra i quali, per esempio, Outlook Express, Eudora, IncrediMail, Mozilla Thunderbird ecc.

◀ Client di posta Viene anche chiamato Mail User Agent (MUA e verrà descritto in seguito) e si tratta di un programma molto diffuso che consente di comporre, inviare, ricevere e organizzare i messaggi di posta elettronica da e verso il server di posta elettronica di un ISP (*Internet Service Provider*) al quale siamo registrati. ▶

La Web mail invece consente di accedere alla casella di posta elettronica solo attraverso la connessione a un sito dedicato a questo scopo come, per esempio, Hotmail, GMail ecc. La seguente tabella ne illustra le principali caratteristiche.

Web mail	POP mail
Gratuita	Spesso a pagamento
Accesso da qualunque computer con connessione a Internet	Accesso solo da computer nel quale è installato il programma di posta elettronica (client)
Necessità di ricordare la password a ogni accesso	Password memorizzata solo durante la creazione dell'account
Metodo poco sicuro, le password possono essere intercettate	Metodo sicuro in quanto le password sono memorizzate nel computer client
Gli allegati sono consentiti solo se sono di dimensioni limitate	Gli allegati possono essere di dimensioni molto elevate
Rischio di ricevere molte email indesiderate (spam)	Rischio spam ridotto

Invio e ricezione di posta elettronica

Dopo aver scritto una email utilizzando un qualunque programma di posta con l'indicazione dell'indirizzo del destinatario, provvediamo a inoltrarla sulla rete.

Analogamente al sistema postale cartaceo, non è necessario che il ricevente sia connesso alla rete e abbia in funzione anch'esso un programma di posta elettronica: al momento della trasmissione della posta da parte del mittente il destinatario potrebbe essere impegnato oppure avere il computer spento.

La email non raggiunge quindi immediatamente il computer del destinatario, ma viene depositata in una memoria, come nel "fermo posta" degli uffici postali, in attesa che qualcuno la "passi a ritirare."

Vediamo dettagliatamente come avviene il trasferimento dei messaggi di posta elettronica tra gli intermediari, così come è stato definito in RFC 822: viene utilizzato il protocollo Simple Mail Transfer Protocol (SMTP).

La realizzazione della posta elettronica viene implementata mediante due sottosistemi:
- Mail User Agent (MUA);
- Mail Transport Agent (MTA).

MUA

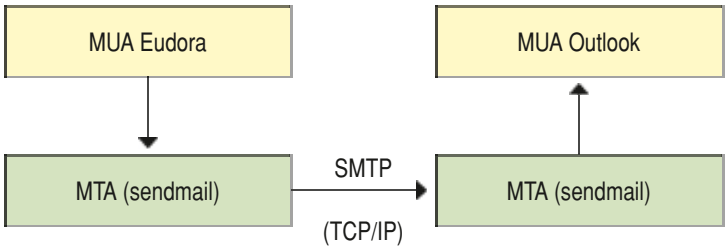
Il MUA, come già detto precedentemente, è un programma di gestione di posta che viene mandato in esecuzione sul client e mediante una interfaccia grafica user friendly offre all'utente le funzionalità che permettono l'inserimento, la composizione, la ricezione e la lettura dei messaggi.

> Come vedremo, i messaggi devono essere strutturati secondo una sintassi di composizione definita nel RFC 822 e nel MIME.

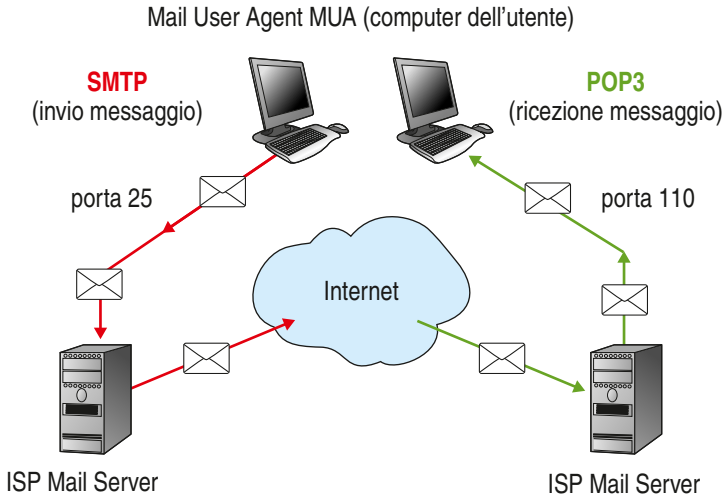
Per spedire i messaggi MUA utilizza il protocollo SMTP e li consegna a un programma MTA che si occupa della trasmissione al MUA destinatario.

MTA

L'MTA si occupa della ricezione di tutti i messaggi e del loro recapito e ha quindi la funzione di ponte tra due MUA: è quello che noi indichiamo come mailserver.
Può essere paragonato a una centralina telefonica dove vengono smistate le chiamate in ingresso e in uscita, e offre i seguenti servizi:
- server SMTP (porta 25): gestisce la spedizione e la ricezione dei messaggi tra server SMTP;
- server POP3 (porta 110): gestisce la spedizione dei messaggi al client;
- server IMAP4 (porta 143): permette la gestione dei messaggi sul server dal client.



Il MUA è quindi una applicazione in esecuzione su un server dell'ISP dell'utente: questo compone e invia il messaggio verso il proprio ISP che si occupa della ricezione di tutti i messaggi e del loro recapito al mail server dell'IPS di destinazione, raggiungibile dal destinatario del messaggio.
Lo schema completo di trasmissione e ricezione è riportato nella seguente figura.



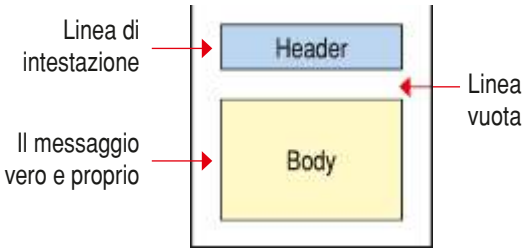
I mail server hanno al loro interno la mailbox "fermo posta" degli utenti contenente i messaggi in entrata che non sono ancora stati letti e scaricati sui rispettivi client nel caso di gestione in modalità POP mail: nel caso di Web mail al MTA vengono aggiunte anche tutte le funzionalità del sottosistema MUA dato che l'utente effettua tutte le operazioni direttamente sul server.
Inoltre, per entrambe le situazioni, i mail server hanno memorizzato la coda dei messaggi in uscita contenente i messaggi non ancora recapitati.
L'invio del messaggio da parte del client mail avviene utilizzando il protocollo SMTP mentre la ricezione viene effettuata con il protocollo POP3.

Il protocollo SMTP

Il primo documento che descrive il protocollo per la rappresentazione dei documenti di posta elettronica è l'RCF 822, del 1982; in esso viene specificato il formato per i messaggi di posta ma limitandosi ai messaggi di testo, cioè esclusivamente a simboli (caratteri) di 7 bit in formato ASCII, senza fare alcun riferimento ad altri contenuti come per esempio le immagini.

Il formato del messaggio

L'RCF 822 è una stringa di testo costituita da un header e da un body separati da una linea vuota. ▶
L'header contiene le informazioni per il trasporto:



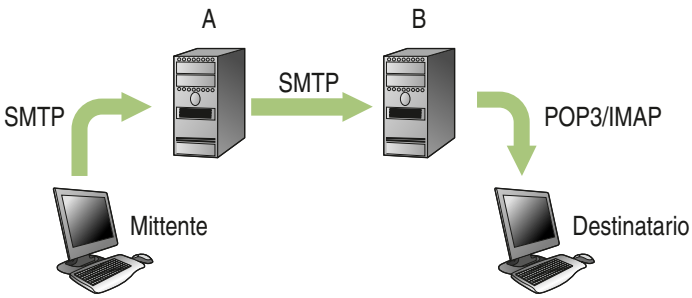
To:	lista di destinatari
From:	mittente
Cc:	lista di destinatari per conoscenza
Bcc:	lista nascosta di destinatari per conoscenza
Date:	data di spedizione
Reply-to:	indirizzo diverso dal mittente
Subject:	titolo del messaggio

Il body, che è il "messaggio vero e proprio", è costituito da soli caratteri ASCII: nel caso ci fosse bisogno di trasmettere un messaggio costituito non solo da testo ASCII, deve prima essere convertito in questo formato per poter poi essere inviato in rete; inoltre i caratteri ASCII trasportati dal SMTP sono a 7 bit e quindi sono solo i primi 128 mentre all'interno di un file binario possono essere contenuti tutti i 256 caratteri possibili.

Con lo standard MIME è possibile inserire in un qualsiasi messaggio di email, oltre al testo, anche file contenenti immagini, segnali audio e video; il software di gestione della posta si limita a "trasferire" il file al destinatario senza analizzarne il contenuto, che sarà interpretato e decodificato dall'utente che lo utilizzerà in base alle specifiche di tipo inserite nel messaggio stesso.

Trasferimento SMTP

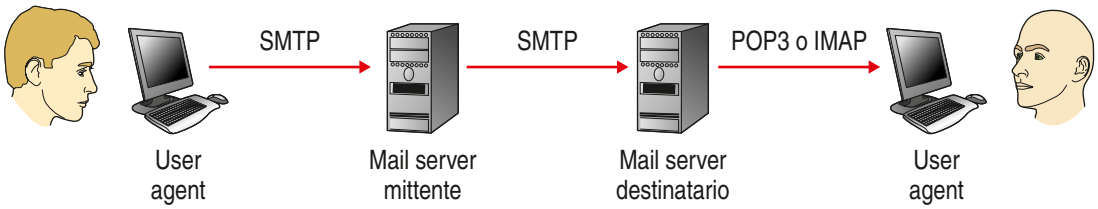
Il protocollo SMTP usa il protocollo TCP (porta 25) per consegnare in modo affidabile messaggi dal client al server (l'utilizzo della porta 25 è indicata dalla RCF 1060: "smtp 25/tcp mail").
L'invio di un messaggio dal mittente al destinatario è composto da tre fasi che coinvolgono i rispettivi server di posta del mittente (A) e del destinatario (B):



1. Il programma di posta elettronica usato dall'utente invia il messaggio al proprio server (A) usando il protocollo SMTP.
2. Il server trasferisce il messaggio al server del destinatario (B) utilizzando lo stesso protocollo:
   - A, sulla base dell'indirizzo email del destinatario, identifica il server B e apre una connessione;
   - B identifica il nodo di rete da cui proviene la connessione (cioè il suo indirizzo IP) e accetta la connessione; memorizza inoltre tale identificazione come parte iniziale del messaggio da ricevere;
   - A comunica l'username del destinatario;
   - B verifica la validità dell'indirizzo e autorizza la trasmissione del messaggio;
   - A invia il messaggio e chiude la trasmissione;
   - B memorizza il messaggio in attesa che il reale destinatario si colleghi e ritiri il messaggio utilizzando un apposito protocollo (solitamente POP3 o IMAP).
3. Il destinatario preleva il messaggio dal proprio server.

Prelievo della posta: Post Office Protocol (POP3)

Fino a ora abbiamo visto il trasferimento dei messaggi tra i vari mail server: ora analizziamo come un utente possa, in un momento qualsiasi, accedere alla propria casella di posta elettronica per leggere i propri messaggi scaricandoli sul disco del proprio PC locale.
Questa operazione viene effettuata mediante il protocollo Post Office Protocol (POP) che permette a un client di posta di accedere al server ed effettuare il trasferimento dei messaggi dalla propria mailbox ("fermoposta") al proprio PC, nel programma client di posta che è installato su di esso.



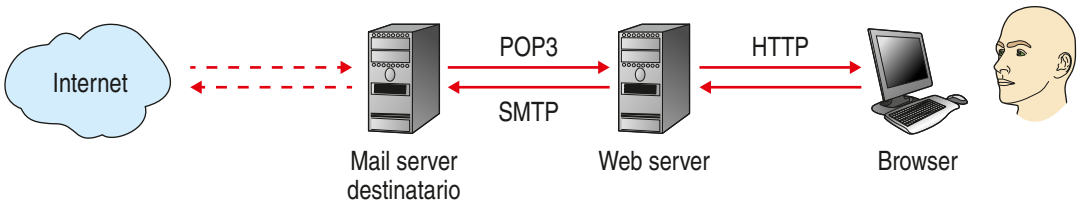
POP3 è un sistema molto semplice che all'avvio del client di posta effettua il log-on al mail server del destinatario e scarica tutti i messaggi a esso pervenuti dai mail server mittenti dall'ultima connessione stabilita: contemporaneamente ai messaggi in arrivo scarica anche gli eventuali attachment a essi collegati.

> Il protocollo POP è anch'esso un comune protocollo client/server dove lo user agent ha ancora il ruolo di client POP e il mail server ha il ruolo di server POP.

La conversazione POP3, che utilizza la porta 100, avviene in tre fasi:
- autorizzazione (AUTHORIZATION): il client si identifica e il server verifica che abbia le dovute autorizzazioni per accedere alla casella postale;
- transazione (TRANSACTION): è la fase nella quale la posta viene effettivamente scaricata e al termine della stessa il client lancia il comando QUIT;
- aggiornamento (UPDATE): in questa fase il server elimina dalla casella postale tutti i messaggi scaricati e chiude la connessione.

L'accesso alla posta via WEB (Web mail)

La seconda modalità di consultazione della posta è quella che viene offerta direttamente dai siti Web che offrono l'accesso alle proprie caselle di posta (Hotmail, GMail, libero, inwind, tin, Yahoo! ecc.) attraverso la connessione a un sito dedicato a questo scopo direttamente con il browser: in questo caso la posta non può essere scaricata sul client ma viene consultata e scritta direttamente in rete sul Web server.



Protocollo IMAP

Un protocollo alternativo al POP3, ancora poco diffuso nonostante sia molto più evoluto, è l'Internet Message Access Protocol (IMAP), particolarmente utile per gli utenti "remoti o mobili".

> Il principale vantaggio di IMAP è quello di permettere l'accesso alla posta sia online che offline e di consentire alcune manipolazioni avanzate sulla posta in entrata prima ancora di prelevarla dal server.

Il protocollo IMAP, che opera sulla porta 143, consente inoltre di:
- rinominare la propria casella elettronica;
- cancellare singoli messaggi senza essere costretto a prelevarli;
- leggere le intestazioni dei messaggi senza doverli prelevare interamente;
- prelevare addirittura solamente delle porzioni dei messaggi;
- effettuare l'acceso simultaneo alla stessa casella di posta.

La versione più recente, l'IMAP4, è candidata a diventare lo standard di riferimento su Internet e permette inoltre all'utente di archiviare i messaggi in cartelle direttamente sul server, di accedere contemporaneamente a più mail server e di condividere le mailbox con altri mail server.
Offre inoltre una migliore integrazione con la tecnologia MIME che viene usata per effettuare gli attachment ai messaggi.

Nome simbolico e indirizzo IP

Per identificare un host oppure un router in Internet sappiamo che è necessario conoscere il suo indirizzo IP, che è unico sulla rete pubblica: ma un sito Internet è generalmente individuato da un nome mnemonico, che è più semplice utilizzare da parte dagli "esseri umani".

> È decisamente più facile ricordare www.hoepli.it piuttosto che il suo indirizzo IP 193.202.13.14.

Anche ai PC di una LAN viene generalmente associato un nome simbolico che però deve essere mantenuto in corrispondenza del rispettivo indirizzo IP: in una rete locale questo può essere fatto con un semplice "file hosts" composto da coppie di dati, come nel seguente esempio:
- 192.168.1.1 Contabilità_1
- 192.168.1.2 Contabilità_2
- 192.168.1.3 Magazzino_1
- 192.168.1.4 Magazzino_2
- 192.168.1.5 Vendite_1
- 192.168.1.6 Server
- …

ma al crescere della dimensione della rete e quindi del numero di host questa soluzione è impraticabile.

> Capita anche di assegnare allo stesso host più di un nome simbolico: siamo in presenza quindi di alias.

In Internet la risoluzione dei *nomi degli host* in *indirizzi IP* è un servizio che viene effettuato dal Domain Name System (DNS).

DNS

Con Domain Name System si intende:
- un data base distribuito che memorizza coppie (nome simbolico – indirizzo IP) su un insieme di nodi della rete (name servers);
- un protocollo a livello applicazione che regola la comunicazione tra hosts e name servers utilizzato da altri protocolli per la risoluzione dei nomi simbolici.

ESEMPIO

Se inseriamo in un browser (HTTP client) il nome:
http://www.hoepli.it/index.html
Il client HTTP attiva un client DNS che
- estrae dall'URL l'indirizzo simbolico IS del server (hoepli.it);
- interroga il DNS e ottiene l'indirizzo IP corrispondente a IS;
- invia quindi una richiesta (secondo il protocollo HTTP) al Web server (passa l'indirizzo IP al livello TCP).

Quando un server locale non riesce a tradurre il nome simbolico di un sito Web in un indirizzo IP contatta un server DNS radice che se non conosce la mappatura contatta a sua volta un server DNS autorizzato ottenendo la mappatura e restituendola al server DNS locale.

Attualmente esistono sparsi per il mondo *13 server radice* etichettati da A a M organizzati come un cluster di server replicati, e hanno il nome da «a.root-servers.net» a «m.root-servers.net»; sono anche detti *server di nomi radice* e corrispondono ai domini di più alto livello (top-level domain).

I server TLD (Top-Level Domain) sono collegati agli altri server presenti nella rete generando una struttura "ad albero", e comprendono i domini com, org, net, edu ecc. e tutti i domini locali di alto livello, quali uk, fr, ca e jp.

Nomi di primo livello

I nomi di primo livello possono essere classificati in tre gruppi, a seconda della gerarchia di cui sono "a capo":

- gerarchia organizzativa:
  - .arpa corrisponde ai terminali derivanti dalla rete originale;
  - .com corrispondevano inizialmente alle aziende a vocazione commerciale.
  - .edu corrisponde agli enti educativi;
  - .gov corrisponde agli enti governativi;
  - .net corrispondeva inizialmente agli enti con tratti di rete;
  - …
- gerarchia geografica:
  - .it domini italiani;
  - .fr domini francesi;
  - .uk domini inglesi;
  - .us domini degli Stati Uniti;
  - …
- gerarchia generica:
  - .museum corrisponde ai musei;
  - .aero corrisponde all'industria aeronautica;
  - .biz (business) corrisponde alle aziende commerciali;
  - .coop corrispondente alle cooperative;
  - .info corrisponde agli enti con tratti di informazione;
  - .name corrisponde a nomi di persone o a nomi di personaggi immaginari.

Una seconda metodologia di classificazione "più formale" raggruppa i domini in due categorie:

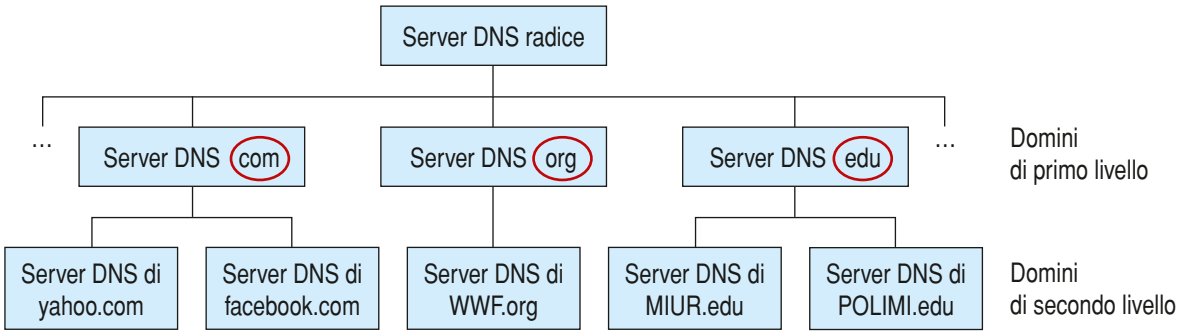
1. i domini detti "generici", chiamati gTLD (*generic TLD*), classificati in base al settore di attività, a loro volta suddivisi in tre gruppi:
   - gTLD storici:
     - .arpa, .com, .edu, .gov, .int, .mil, .net, .org
     - gTLD nuovi introdotti nel novembre 2000 dall'ICANN:
     - .aero, .biz, .museum, .name, .info, .coop, .pro
   - gTLD speciali:
     - .arpa
2. I domini detti "nazionali", chiamati ccTLD (*country code TLD*) sono uno per ogni Paese e i loro nomi corrispondono alle abbreviazioni dei nomi degli Stati definiti dalla norma ISO 3166.

Al livello inferiore ogni nodo dell'albero viene detto "nome del dominio" e può essere al massimo lungo 63 caratteri: vengono definiti nomi di secondo livello e possono essere di due tipi:

- in alcune gerarchie prevedono semplicemente il nome dell'organizzazione, come .enel.it, .rai.it ecc.;
- in altre prevedono prima una caratterizzazione .bt.co.uk.

ESEMPIO

Un esempio di albero è il seguente:



L'estremità di un ramo (foglia) è detta host e corrisponde a un terminale o a un'entità di rete: il nome simbolico che viene attribuito all'host deve essere unico nel dominio considerato (generalmente gli viene assegnato il nome www).
Oltre ai domini di secondo livello possono esistere altri livelli inferiori, chiamati sottodomini.

Il numero di livelli di sottodomini è variabile è può arrivare fino a un valore massimo di 127.

Anche ogni nodo dell'albero ha un nome di dominio che si ottiene dalla sequenza di etichette separate da punti (.) ottenute scorrendo il ramo dalla foglia alla radice, come per esempio www.milano.hoepli.it; ogni punto separa un nodo e concatena da sinistra verso destra le label associate ai vari nodi a partire da quello in questione fino alla radice.

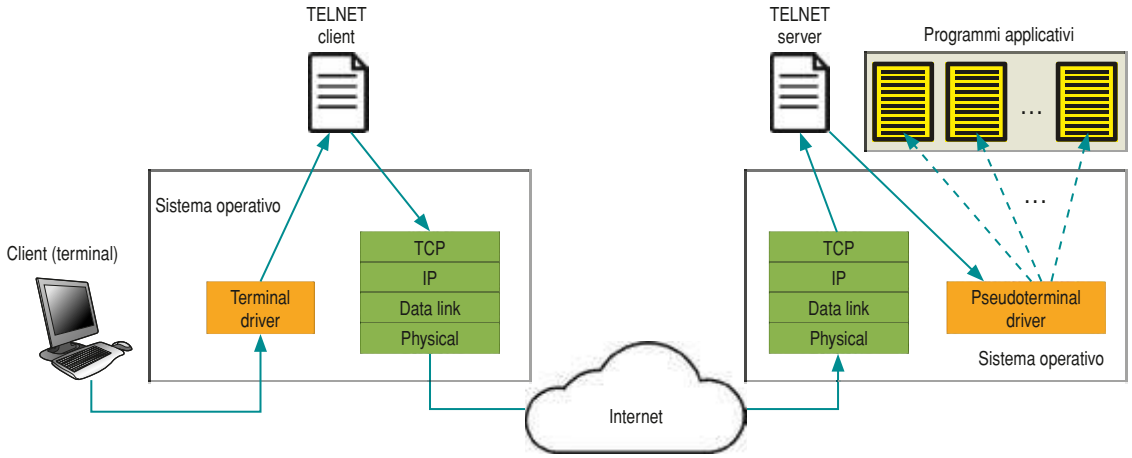
L'ultima etichetta è quella della radice, che è una stringa nulla: quindi tutti i nomi di dominio terminano con un punto.

Telnet

Telnet è un protocollo applicativo client-server basato su TCP, che permette di aprire una sessione di comunicazione non criptata e bidirezionale tra due host. Una volta realizzata la connessione, il client può lavorare sulla macchina remota come se fosse direttamente collegata al proprio computer. Eseguendo il comando Telnet dal computer client, viene richiesta una connessione sul server tramite la porta 23, e contemporaneamente sul server deve essere in esecuzione un programma in ascolto sulla porta 23.
La sintassi di un comando Telnet sul client è la seguente :

```
telnet [<opzioni>] [<host-remoto> [<porta>]]
```

La sessione aperta dal comando Telnet consente di utilizzare solo comandi richiamabili da linea di comando, o che comunque non necessitano di interfaccia grafica.



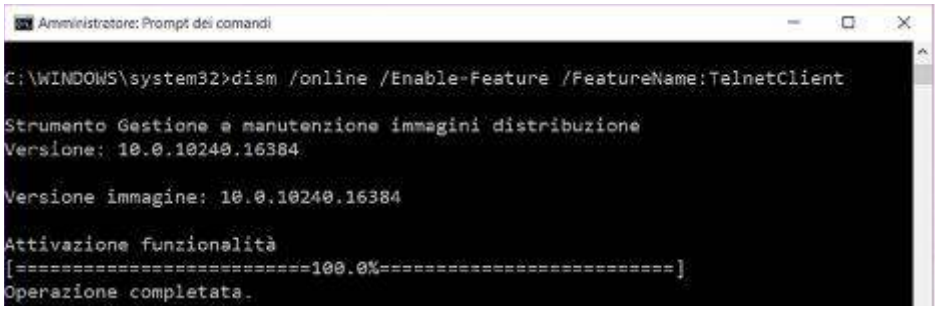
Su Windows 10 possiamo attivare Telnet, sia come servizio client che come server, attraverso la seguente procedura:

1. Nella casella di ricerca digitiamo cmd.exe, quindi col tasto destro del mouse, clicchiamo sulla voce Esegui come amministratore. Chiudiamo con un Sì la finestra Controllo dell'account utente, come indicato nell'immagine alla pagina seguente.

2 Nella nuova finestra a linea di comando che appare digitiamo il comando seguente:

```
dism /online /Enable-Feature /FeatureName:TelnetClient
```

e premiamo Invio per confermare l'installazione del client.



3 Una volta installato il client appare il prompt Microsoft Telnet> indicante che il sistema è in attesa di comandi Telnet:

Per avviare una sessione Telnet occorre indicare l'host al quale collegarsi; di default la porta utilizzata è la porta 23, ma è anche possibile indicarne una diversa mediante la linea di comando:

```
telnet nomehost
```

oppure

```
telnet nomehost 35
```

La comunicazione avviene mediante un protocollo bidirezionale half-duplex codificato a 8 bit e il flusso di dati viene inviato linea per linea: il byte che segue un valore 255 viene interpretato come un comando.

Sostanzialmente abbiamo quattro tipi di richieste:

- vuole usare (`DO`);
- rifiuta di usare (`DON'T`);
- vuole che l'altra estremità usi (`WILL`);
- rifiuta che l'altra estremità usi (`WON'T`).

Ogni richiesta è seguita da un numero che indica il tipo di opzione, come per esempio:

`WILL XXX`

indica che un partner desidera usare l'opzione XXX;

`DO XXX` e `DON'T XXX`

saranno gli acknowledgments (riconoscimenti della richiesta) positivo e negativo. Nel caso opposto, il comando `WON'T XXX` indica che un partner non desidera più usare l'opzione XXX.

Il comando
`DO XXX`
indica che un partner richiede all'altro partner di usare l'opzione XXX;
`WILL XXX` e `WON'T XXX`
saranno gli acknowledgments positivo e negativo.
Nel caso opposto, il comando
`DON'T XXX`
indica che un partner richiede all'altro partner di togliere l'opzione XXX. Combinando proposta e risposta otteniamo le possibili situazioni riportate nella seguente tabella:

Richiesta	Risposta	Interpretazione
DO	WILL	L'emittente comincia usando l'opzione
	WON'T	L'emittente non deve usare l'opzione
WILL	DO	L'emittente comincia usando l'opzione, dopo aver inviato un DO
	DON'T	L'emittente non deve usare l'opzione
DON'T	WON'T	L'emittente segnala che ha disattivato l'opzione
WON'T	DON'T	L'emittente segnala che deve disattivare l'opzione

◀ Il NVT (Network Virtual Terminal) è un ambiente virtuale creato ai due estremi della connessione, dove operano rispettivamente il client e il server Telnet: naturalmente i due host possono essere di tipo diverso, con sistema operativo diverso e software Telnet diverso. ▶

Alla base del protocollo Telnet è stato posto il concetto di simmetria, cioè si è scelto un protocollo simmetrico in quanto molto semplice da realizzare: questo però può portare a inconvenienti dovuti proprio al fatto che non essendoci un host prevalente la fase di negoziazione delle opzioni potrebbe portare a un "ciclo infinito" di richieste nel caso di una errata interpretazione di una richiesta. Per prevenire queste possibili situazioni indesiderate, l'◀ NVT ▶ deve seguire queste regole:

- ogni interlocutore può richiedere un solo cambio nelle opzioni;
- non è possibile richiedere lo stato di una opzione;
- se viene inoltrata una richiesta per un'opzione già attiva, questa viene ignorata;
- deve essere inviato un ACK in risposta per ogni richiesta di cambio di stato;
- se viene richiesto il cambio di stato di una opzione che modifica il trattamento dei dati, questo deve essere inserito nel flusso di dati nel punto in cui gli stessi devono essere interpretati diversamente.

ESEMPIO

Supponiamo che l'host A debba spedire i caratteri `X`, `Y`, `Z`, `CR`, `LF`, `1`, `2`, all'host B, ma che voglia spedire gli ultimi due, cioè `1` e `2`, subito, senza aspettare il prossimo `end of line`; è possibile farlo in questo modo:

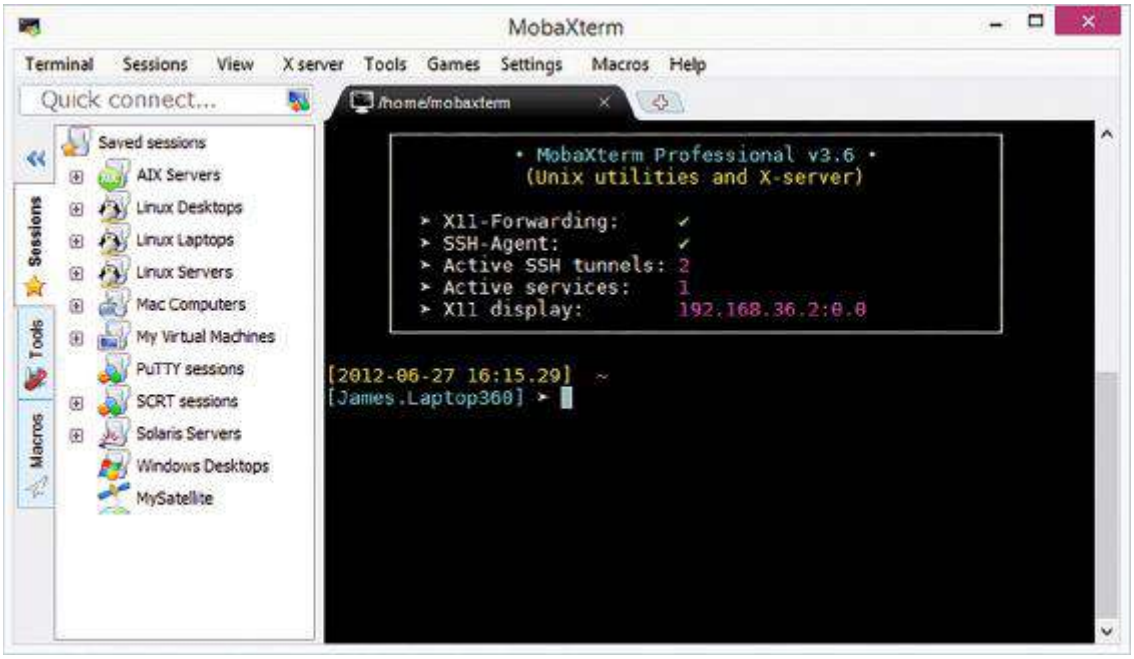
- prima si spediscono i caratteri `X`, `Y`, `Z`, `CR`, `LF` e si memorizzano in un buffer i caratteri `1` e `2`;
- quindi si inviano due richieste di opzioni `DO ECHO` e `DO SUPPRESS-GO-AHEAD` per informare l'host B che l'output seguente sarà del tipo char-at-time;
- l'host B risponde con `WILL ECHO` e `WILL SUPPRESS-GO-AHEAD`;
- alla ricezione dei due `ACK`, come conferma delle due richieste di opzione, si spedisce il carattere `1` e `2`;
- ora ogni carattere, non appena verrà processato, verrà spedito.

L'uso principale di Telnet avviene nelle fasi di debug di servizi di networking come i server SMTP e HTTP, in quanto rappresenta un modo semplice per mandare comandi al server ed esaminare le risposte, e nei giochi in rete.

Telnet è stato ormai abbandonato a favore di un nuovo protocollo più sicuro, l'SSH, che, poiché offre tutte le funzioni di Telnet più una sicura criptazione e un'autenticazione a chiave pubblica, è diventato uno standard di fatto per l'amministrazione remota.
La sintassi della linea di comando SSH (Secure Shell) è la seguente:

```
ssh [opzioni] nomeutente@host [comando]
```

La sicurezza della comunicazione tramite SSH è assicurata grazie alla realizzazione di un canale criptato che permette di proteggere da intercettazione i dati scambiati tra client e server. L'intera comunicazione su tale canale avviene in maniera cifrata: SSH realizza cioè sia la mutua autenticazione (del client e del server) che la protezione della comunicazione durante l'intera sessione di lavoro. Esistono software che consentono la connessione a un server che può essere amministrato da remoto tramite protocollo sicuro SSH, come ad esempio MobaXterm.



Verifichiamo le conoscenze

1. Risposta multipla

1 In Internet, l'indirizzo di posta elettronica è del tipo:

a. nomeutente@dominio
b. dominio @destinatario
c. dominio @utente
d. indirizzo@dominio

2 MAU è l'acronimo di:

a. Mailbox User Acces
b. Mailbox User Agent
c. Mail Utent Agent
d. Mail Utent Acces
e. Mail User Agent

3 Quali tra le seguenti affermazioni sono false?

a. Il POP mail utilizza il protocollo SMTP per l'inoltro dei messaggi
b. Il POP mail utilizza il protocollo POP3 per l'inoltro dei messaggi
c. La Web mail utilizza il protocollo SMTP per l'inoltro dei messaggi
d. La Web mail utilizza il protocollo POP3 per l'inoltro dei messaggi
e. Il POP mail utilizza il protocollo SMTP per la ricezione dei messaggi
f. Il POP mail utilizza il protocollo POP3 per la ricezione dei messaggi
g. La Web mail utilizza il protocollo SMTP per la ricezione dei messaggi
h. La Web mail utilizza il protocollo POP3 per la ricezione dei messaggi

4 Con Domain Name System si intende:

a. un data base distribuito che memorizza coppie di dati (nome simbolico – indirizzo IP)
b. un data base distribuito che memorizza coppie di dati (nome simbolico – indirizzo router)
c. un protocollo a livello applicazione che regola la comunicazione tra hosts e router
d. un protocollo a livello applicazione che regola la comunicazione tra router e name servers
e. un protocollo a livello applicazione che regola la comunicazione tra hosts e name servers

5 Le tre funzioni principali del DNS sono (indicare quella inesatta):

a. tradurre dei nomi in indirizzi
b. gestire gli alias
c. individuare i domini
d. eseguire il bilanciamento del carico

6 La soluzione di avere un unico database per il DNS è irrealizzabile perché:

a. diventa un single point of failure
b. il traffico lo farebbe collassare
c. avrebbe dimensioni troppo elevate
d. sarebbe spesso troppo distante e irraggiungibile
e. sarebbe troppo lento
f. sarebbe permanentemente in manutenzione

7 Quale tra i seguenti non è un dominio di alto livello?

a. .info
b. .rcf
c. .usa
d. .edu
e. .biz
f. .gov
g. .it
h. .rip
i. .arpa
j. .name

8 L'acronimo NVT deriva da:

a. Network Virtual Transport
b. Network Virtual Terminal
c. Natural Virtual Transport
d. Natural Virtual Terminal

9 Quale delle seguenti affermazioni relative al NVT è falsa?

a. Si può accedere a tutti gli host usando la stessa interfaccia (minimale)
b. Consente di collegarsi a un host remoto e operare come se si fosse in locale
c. L'input è gestito dalla tastiera locale
d. L'output è visualizzato sul monitor locale
e. L'echo è visualizzato sul monitor remoto
f. La computazione è effettuata sull'host remoto

10 Il protocollo Telnet si basa su tre concetti fondamentali (indica quello errato):

a. il paradigma del terminale virtuale di rete
b. il principio di opzioni negoziate
c. il principio di bidirezionalità
d. la simmetria del collegamento

11 Nella negoziazione abbiamo quattro tipi di richiesta (indica quella errata):

a. DO
b. WIN
c. DON'T
d. WON'T

12 La sequenza DON'T WON'T:

a. è errata dato che una richiesta non è contemplata
b. indica che l'emittente ha disattivato l'opzione
c. indica che l'emittente non deve utilizzare l'opzione
d. è impossibile
e. indica al ricevente di disattivare l'opzione
f. indica che l'emittente deve disattivare l'opzione

2. Vero o falso

1 L'indirizzo di posta elettronica è associato a una persona. V F
2 POP mail è sinonimo di Web mail. V F
3 Outlook Express, Eudora, IncrediMail, Mozilla sono server mail. V F
4 Il protocollo SMTP è stato definito in RFC 812. V F
5 A ogni host corrisponde un unico indirizzo IP. V F
6 Un host locale non può avere più di un nome simbolico. V F
7 Il servizio DNS funziona attraverso lo scambio di messaggi TCP sulla porta 53. V F
8 Il DNS viene realizzato con un database gerarchico distribuito. V F
9 I server di nomi radice sono 15 etichettati da A a M. V F
10 Le versioni odierne dei sistemi operativi hanno installato di default il client Telnet. V F
11 Le versioni odierne dei sistemi operativi hanno attivato di default il client Telnet. V F
12 Per avviare una sessione Telnet occorre indicare la porta alla quale connettersi. V F
13 Il NVT è un ambiente virtuale creato alla estremità client della connessione. V F
14 NVT definisce un terminale di rete virtuale che fornisce un'interfaccia standard. V F
15 Le conversioni di dati sono problemi locali che non coinvolgono Telnet. V F
16 La fase di negoziare le opzioni potrebbe portare a un "ciclo infinito" di richieste. V F
17 Al codice di escape è stato assegnato il valore decimale 155. V F
18 I comandi di negoziazione delle opzioni sono formati da una sequenza di due byte. V F
19 SSH offre una sicura criptazione e un'autenticazione a chiave pubblica. V F

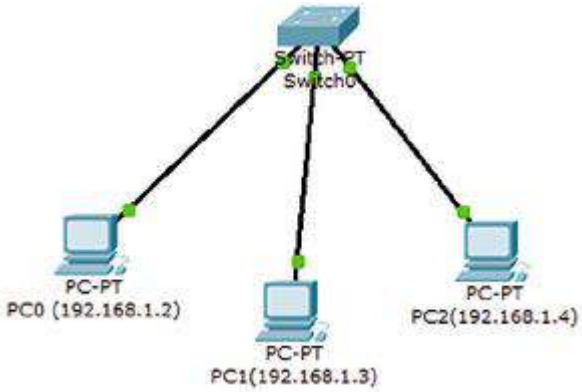
Esercitazioni di Laboratorio 1

SERVER DNS E HTTP CON PACKET TRACER

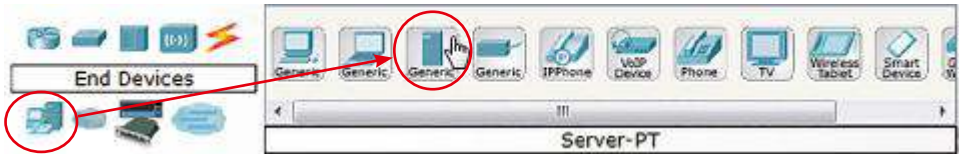
DNS Server

Secondo il modello TCP/IP, mediante il protocollo DNS (Domain Name System) i client interrogano il server DNS per ottenere dal nome alfanumerico l'indirizzo IP e viceversa. Per creare un server HTTP è necessario innanzi tutto attivare il DNS per fare in modo che venga risolto il nome del sito nel relativo indirizzo IP.

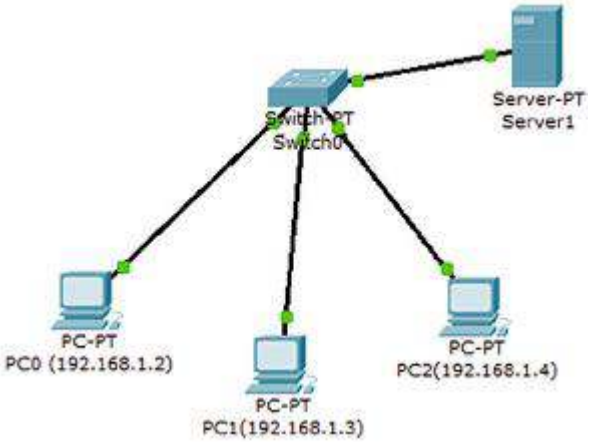
1. Consideriamo la seguente rete dove abbiamo configurato 3 computer (PC-PT) con indirizzi statici, collegati a uno switch come indicato nello schema a fianco:



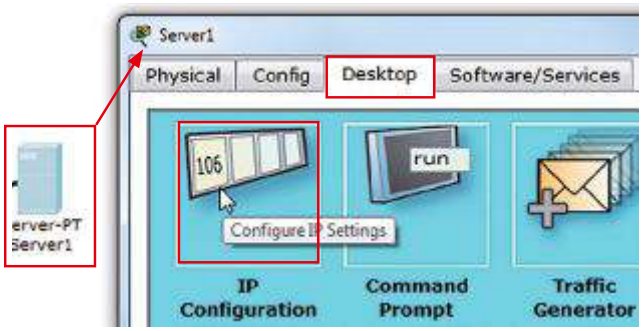
2. Passiamo adesso ad aggiungere un server generico, per fare questo facciamo clic su End Devices, trasciniamo poi l'icona Server-PT, e colleghiamo il server allo switch attraverso Automatically Choose Connection Type.



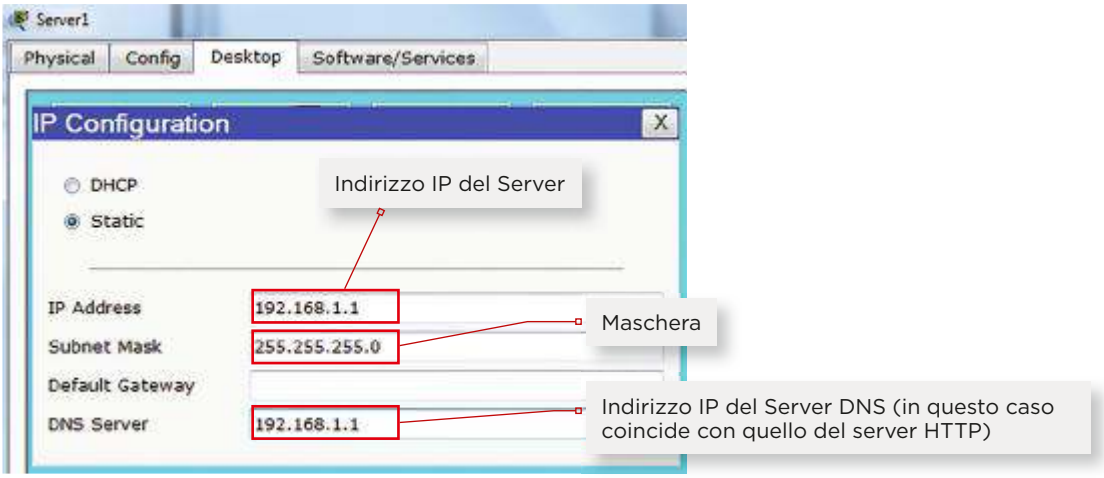
3. Attendiamo che le luci poste ai capi del cavo di connessione diventino verdi:



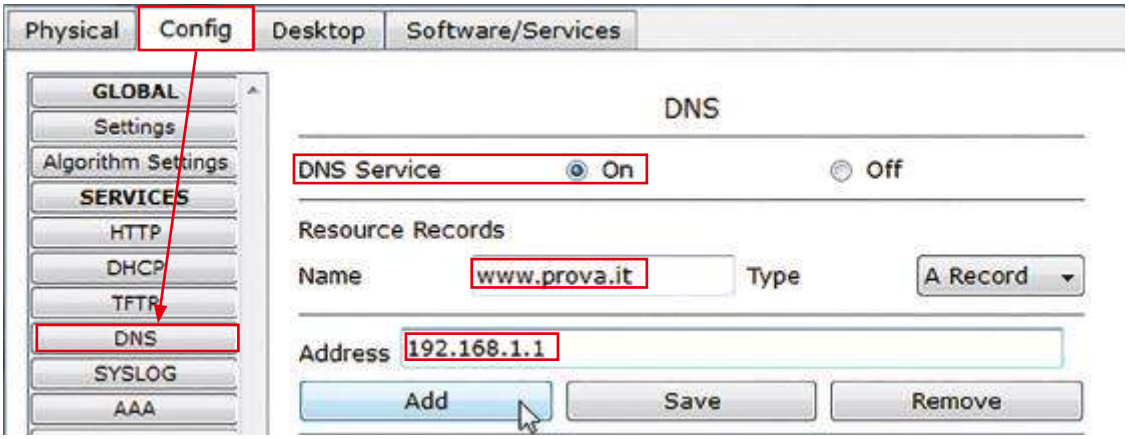
4 Configuriamo il Server-PT: assegniamo un indirizzo statico (192.168.1.1). Per fare questo, dopo aver cliccato sul Server-PT, scegliamo Desktop e quindi IP Configuration:



5 Appare una finestra in cui configurare gli indirizzi come segue:

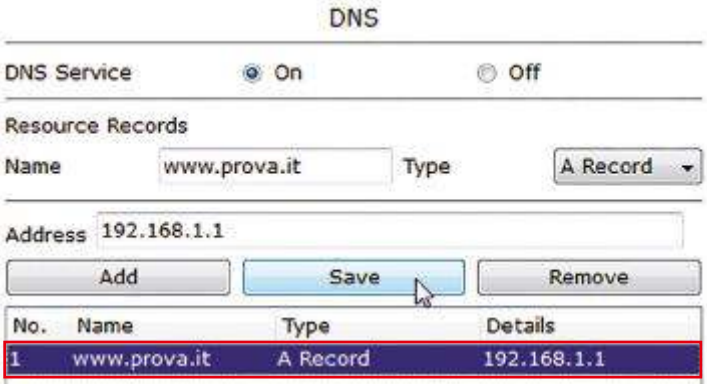


6 Passiamo a configurare il server DNS, per fare questo dobbiamo selezionare la scheda Config, quindi la voce DNS. Associamo al nome simbolico www.prova.it l'indirizzo 192.168.1.1, inserendolo nelle caselle indicate, quindi facciamo clic su Add:

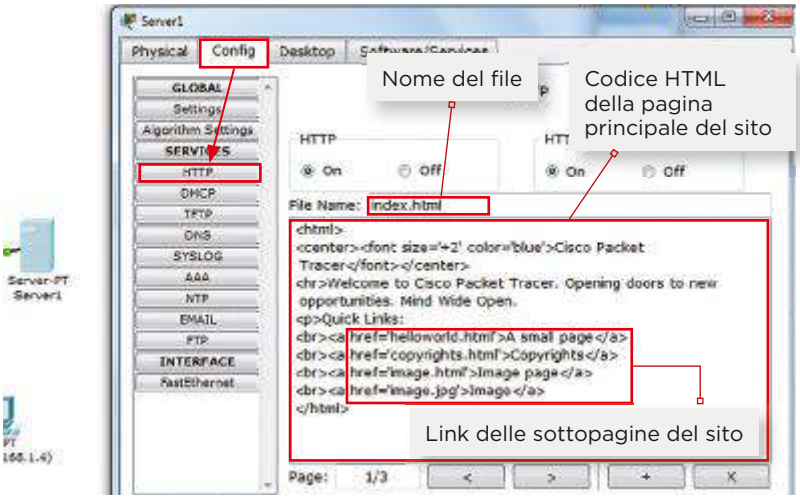


Accanto alla casella del nome (Name) della risorsa che stata inserita, appare un menu a tendina che mostra le voci seguenti:
A Record: restituisce un indirizzo IP, normalmente utilizzato per collegare un nome host al relativo indirizzo IP.
CNAME: consente di collegare un nome DNS con un nome successivo, la risoluzione va avanti con il nuovo nome di tipo CNAME. Consente di far convivere sullo stesso server servizi diversi come ad esempio HTTP, EMAIL, FTP ecc. Ciascun servizio potrà avere il suo riferimento DNS (ad esempio www.prova.it e aula.net per la posta elettronica), oppure quando abbiamo diversi nomi di siti Web allo stesso indirizzo IP.
SOA: restituisce informazioni sul server DNS principale, l'email dell'amministratore, il numero seriale dei timer che regolano la frequenza di trasferimento e la durata di validità dei record.
NS Record: delega una zona DNS a essere gestita da un server DNS autorevole per quel nome di dominio.

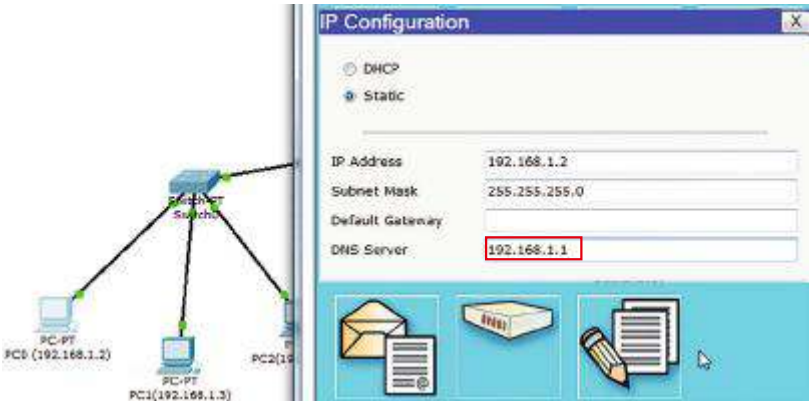
7 Come possiamo notare il nome del sito e il relativo indirizzo IP associato appaiono in elenco. Selezioniamo il nome del sito in elenco (No. 1), quindi su Save per salvarlo nella memoria del server:



8 A questo punto dobbiamo configurare il servizio HTTP sul server, per attivare il Server Web vero e proprio. Per fare questo facciamo clic sull'icona del server, quindi facciamo clic su HTTP nella scheda Config. Come possiamo notare viene mostrato il codice HTML del file che contiene la pagina principale del sito, in questo caso index.html:



9 Adesso dobbiamo definire l'assegnazione dell'indirizzo IP del server DNS a tutti i client della nostra rete. Per fare questo clicchiamo sull'icona del PC-PT e scegliamo la scheda Desktop, quindi IP Configuration. Appare la finestra seguente in cui collocare l'indirizzo del DNS Server (192.168.1.1):



10 Ripetiamo l'operazione eseguita nel punto precedente per tutti i PC della rete, quindi clicchiamo sull'icona del PC-PT e scegliamo la scheda Desktop, quindi Web Browser: ▶

11 Appare la finestra a fianco in cui possiamo digitare l'URL del sito, in questo caso www.prova.it, possiamo vedere che viene aperta la pagina del sito Web: ▶

Prova adesso!

• Applicare un server DNS e HTTP

APRI IL FILE DNS_HTTP.pkt

1. Modifica l'esempio aggiungendo un secondo sito www.esempio.it, modificando il codice HTML del sito stesso a piacere.
2. Verifica il funzionamento della rete aprendo il sito dai diversi computer presenti.
3. Prova ad aprire la pagina principale del sito Web digitando da un computer client l'indirizzo IP del server all'interno della pagina del browser.

Esercitazioni di Laboratorio 2

EMAIL SERVER CON PACKET TRACER

Facciamo comunicare due reti

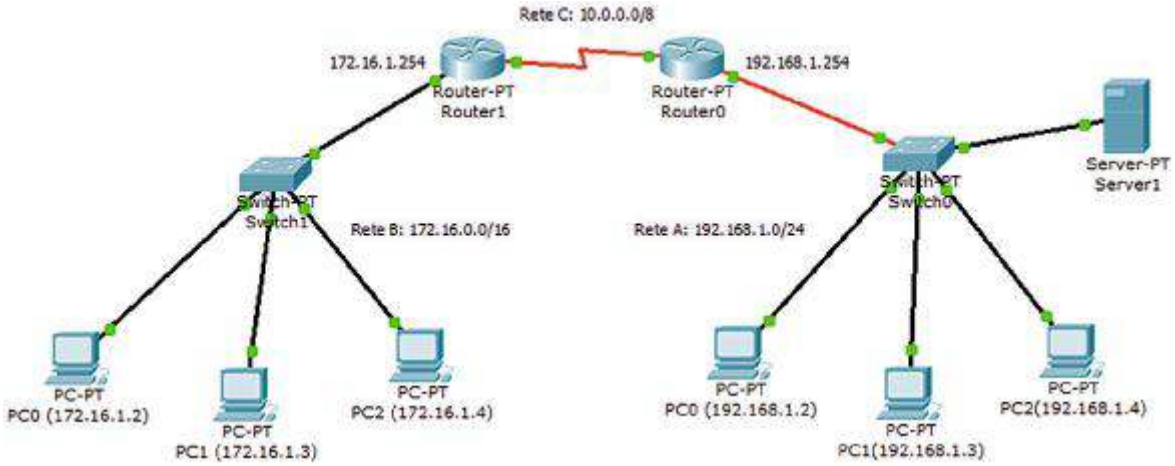
In questa esercitazione vogliamo collocare due router per creare tre reti differenti. In una di queste posizioniamo un server HTTP, dal quale potersi connettere anche dalle altre reti.

Prima di tutto vediamo lo schema generale della rete, ai vari elementi vengono assegnati i seguenti indirizzi IP:

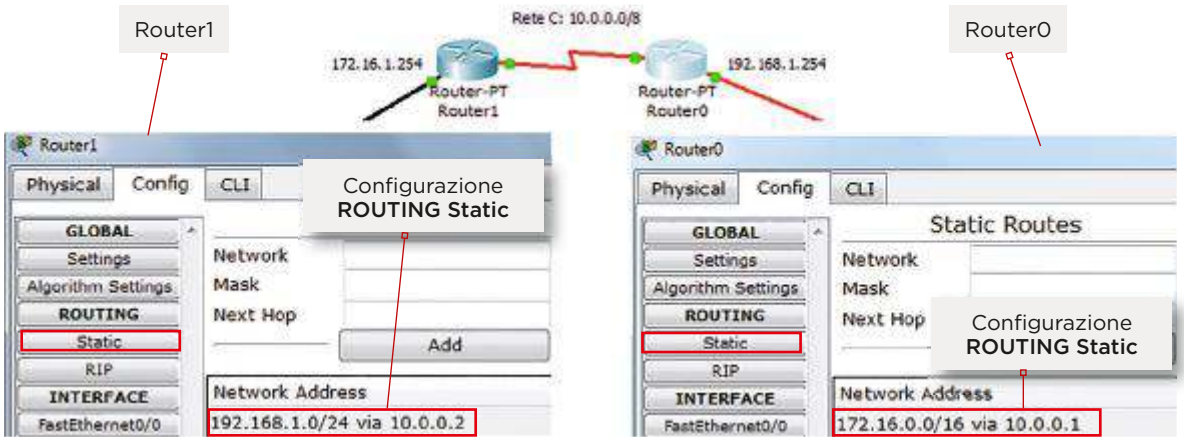
Rete A
3 PC-PT (192.168.1.2/24, 192.168.1.3/24, 192.168.1.4/24)
1 server-PT (192.168.1.1/24)
1 Router (Interfaccia A: 192.168.1.254/24)

Rete B
3 PC-PT (172.16.1.2/16, 172.16.1.3/16, 172.16.1.4/16)
1 Router (Interfaccia B: 172.16.1.254/16)

Rete C
2 Router (10.0.0.1/8, 10.0.0.2/8)



Dopo aver assegnato gli indirizzi IP ai vari PC delle reti e alle interfacce dei router, dobbiamo definire il routing affinché possano essere inoltrati i pacchetti tra le due reti. Per fare questo facciamo clic sui router, quindi Config, ROUTING Static, poi inseriamo i dati come indicato nella figura a pagina seguente.

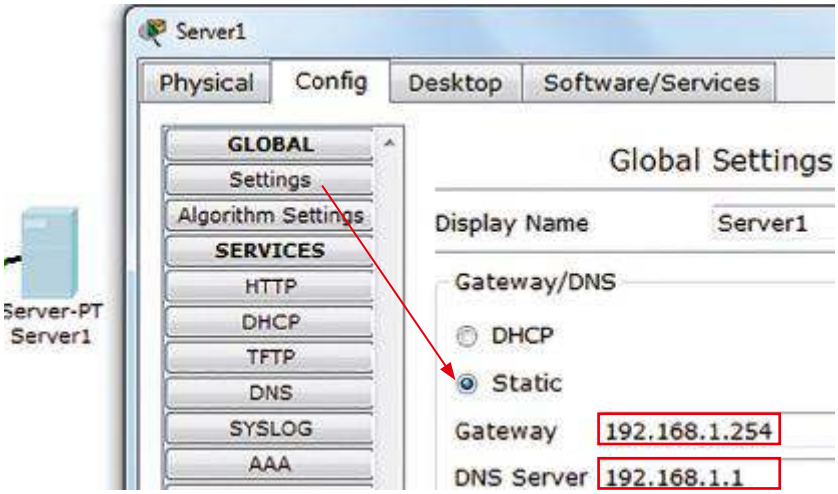


Ricordiamoci di configurare correttamente ciascun PC, assegnando anche l'indirizzo corretto dell'interfaccia interna del router a ogni PC come Gateway. Per i PC della rete A è: (Router0) 192.168.1.254; per i PC della rete B è: (Router1) 172.16.1.254.

Configuriamo il server DNS, HTTP e EMAIL

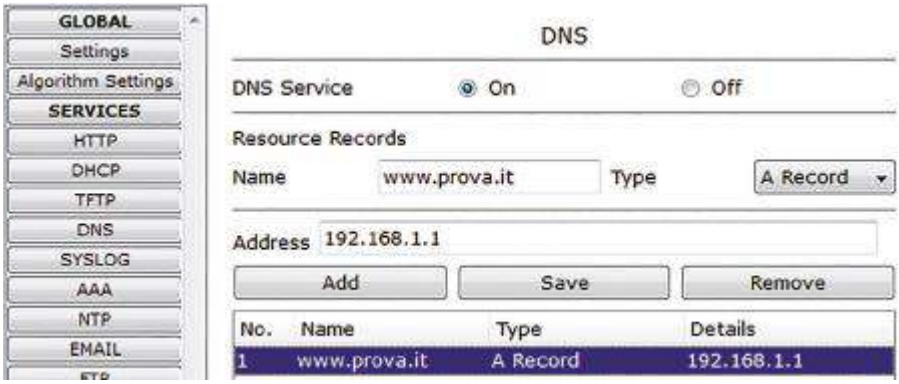
1. Facciamo clic sull'icona del server e attiviamo la scheda Config: assegniamo al server-PT il suo indirizzo IP statico (192.168.1.1).

2. Adesso configuriamo il server di posta elettronica (EMAIL server). Per fare questo prima di tutto dobbiamo definire il servizio DNS per l'utilizzo dei nomi. Inseriamo l'indirizzo del Gateway, rappresentato dall'interfaccia del Router0 (192.168.1.254) e del DNS server (192.168.1.1), rappresentato dall'indirizzo del server stesso.

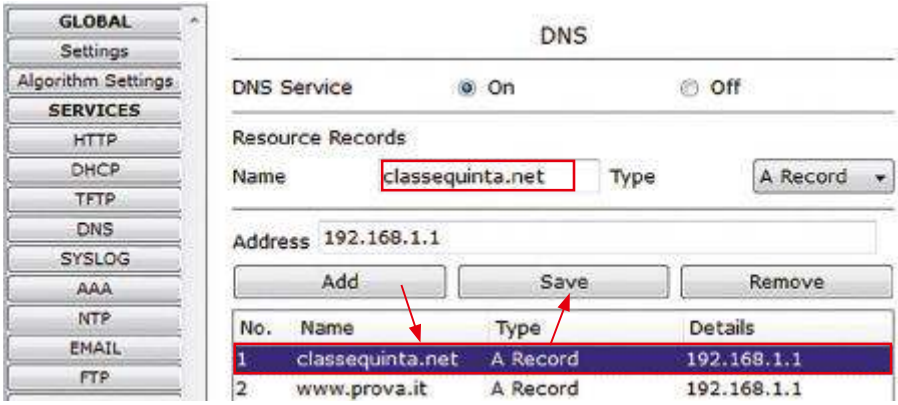


Come possiamo notare il nostro server avrà una triplice funzione, da una parte svolgerà il compito di server DNS, quindi di HTTP server per il sito Web e infine di EMAIL server, come server di posta in arrivo (POP) e in uscita (SMTP).

3 Apriamo la finestra DNS della scheda Config per il server. Aggiungiamo il nome del sito che vogliamo creare (www.prova.it) e salviamolo con il pulsante Save:



4 Passiamo adesso ad aggiungere i nomi utili alla definizione del server di posta elettronica. Per prima cosa definiamo il nome classequinta.net come dominio di posta elettronica, scrivendolo nella casella Name e l'indirizzo 192.168.1.1 nella casella Address; facciamo clic su Add e poi su Save per salvare:



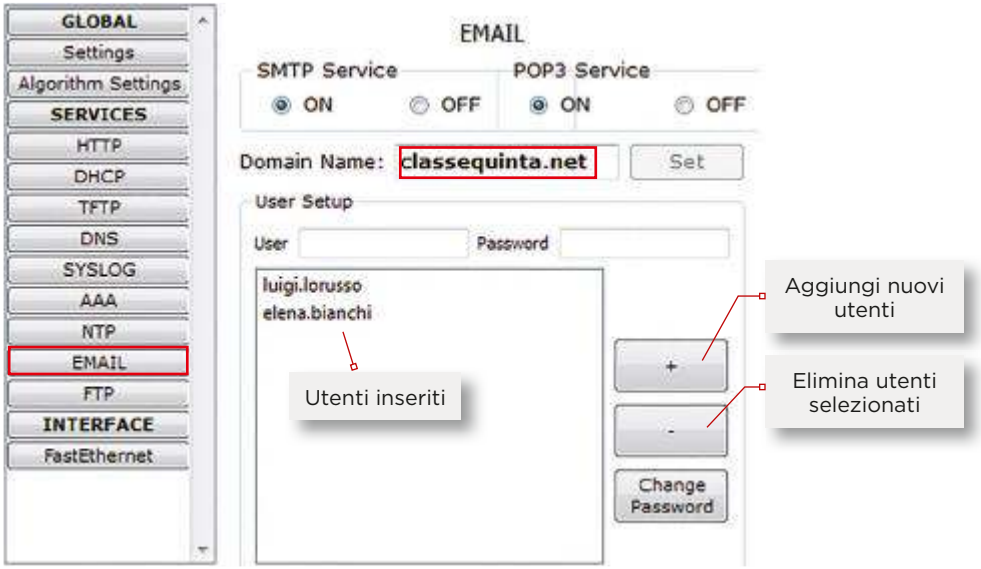
5 Aggiungiamo il nome del server di posta in arrivo (pop.classequinta.net) nella casella Name e scegliamo il tipo CNAME:

6 Ripetiamo la stessa operazione per server di posta in uscita (smtp.classequinta.net) nella casella Name e scegliamo il tipo CNAME:

7 Otteniamo il risultato seguente, dove possiamo notare tutti i nomi che il DNS è in grado di riconoscere:

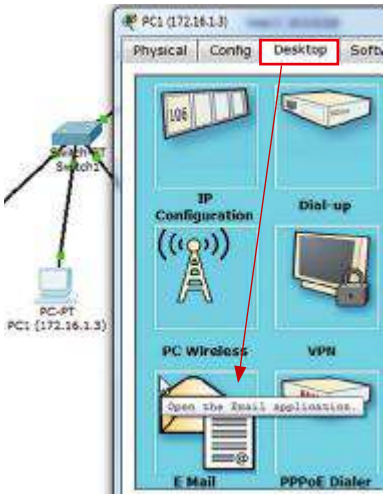
No.	Name	Type	Details
1	classequinta.net	A Record	192.168.1.1
2	pop.classequinta.net	CNAME	classequinta.net
3	smtp.classequinta.net	CNAME	classequinta.net
4	www.prova.it	A Record	192.168.1.1

8 Passiamo adesso alla definizione degli account di posta elettronica. Facciamo clic sul servizio EMAIL quindi, dopo aver compilato la casella Domain Name con il nome del dominio creato nei punti precedenti (classequinta.net), aggiungiamo gli account, in questo caso rappresentati dagli utenti luigi.lorusso e elena.bianchi. Per ciascun account dobbiamo collocare la user name nella casella User e la relativa password nella casella Password, quindi fare clic sul tasto "+":

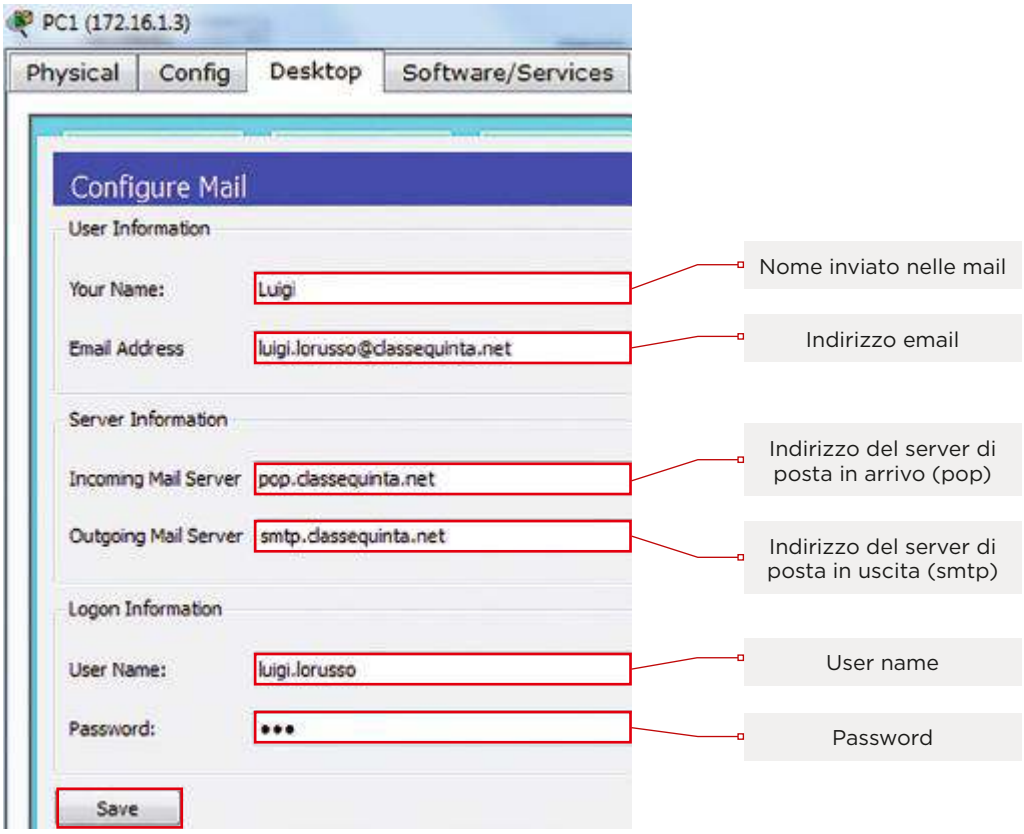


9 Adesso passiamo a configurare il client di posta sui PC. Apriamo un PC a caso della rete B, in questo caso il PC1, quindi aggiungiamo l'indirizzo del server DNS:

10 Adesso passiamo a configurare le impostazioni di posta elettronica. Per definire l'account dobbiamo attivare la scheda Desktop, quindi E-Mail: ▶



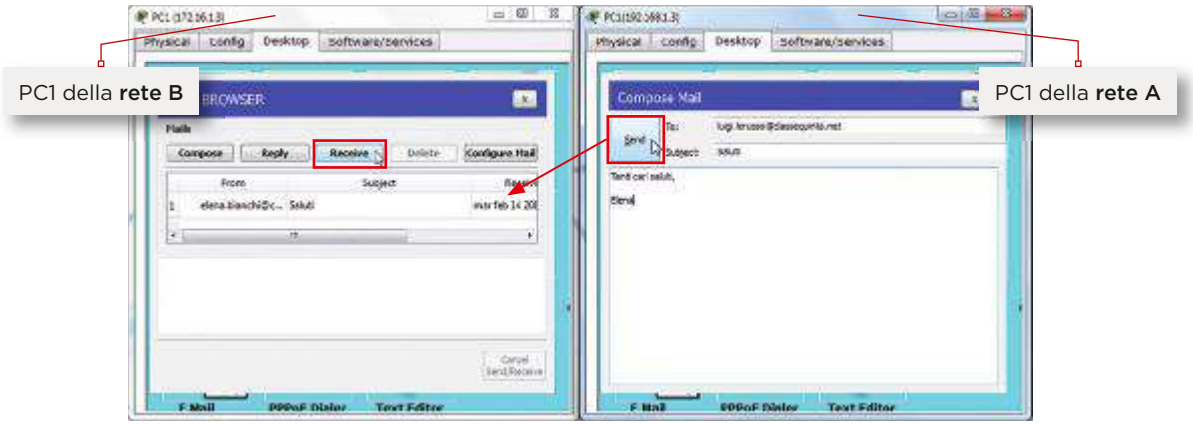
11 Immettiamo nelle caselle relative, le impostazioni dell'account, ricordandoci alla fine di salvare con il tasto Save le informazioni inserite:



12 Ripetiamo le stesse operazioni anche per il PC1 della rete A, inserendo le credenziali dell'utente Elena.

13 Per simulare il funzionamento del sistema procediamo con la composizione di una mail dal PC1 della rete A, facendo clic su Compose: ▶

14 Dopo aver digitato il testo della mail e cliccato su Send, la mail viene inviata al server che provvede a inviarla alla casella del destinatario, in questo caso presente sul PC1 della rete B. Per leggere la posta facciamo clic su Receive: ▼



Prova adesso!

- Applicare un server DNS e HTTP
- Applicare un server Mail

APRI IL FILE DNS_HTTP_Mail.pkt

1. Modifica l'esempio aggiungendo un secondo dominio di posta (classequarta.net) e aggiungendovi un account per ciascun Host della rete.
2. Dopo aver verificato la connessione tra i vari elementi della rete, invia alcuni messaggi email di prova.

Esercitazioni di Laboratorio 3

SERVER FTP CON PACKET TRACER

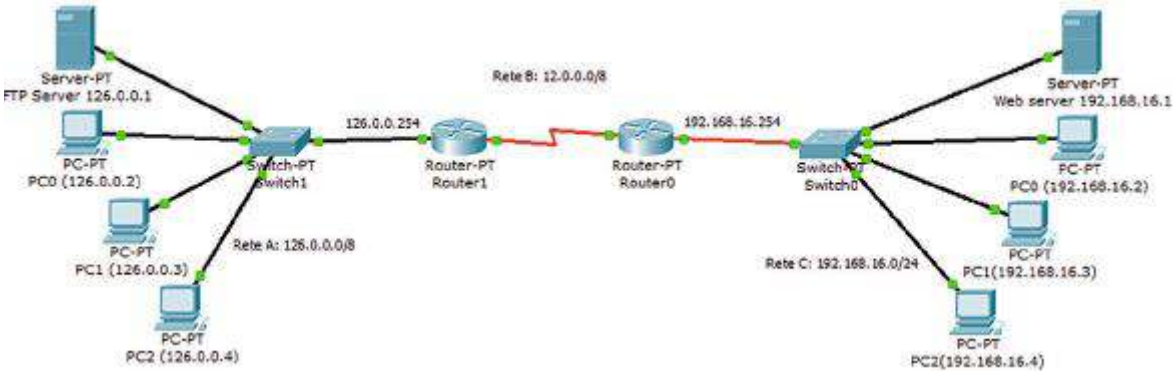
Configurare un FTP server

In questa lezione vogliamo collocare due router per creare tre reti differenti. In una di queste posizioniamo un server FTP, dal quale potersi connettere anche alle altre reti. Vediamo lo schema generale della rete:

Rete A
3 PC-PT (126.0.0.2/8, 126.0.0.3/8, 126.0.0.4/8)
1 FTP server (126.0.0.1/8)
1 Router (Interfaccia A: 126.0.0.254/8)

Rete B
2 Router (12.0.0.1/8, 12.0.0.2/8)

Rete C
3 PC-PT (192.168.16.2/24, 192.168.16.3/24, 192.168.16.4/24)
1 Web server (192.168.16.1/24) e server DNS
1 Router (Interfaccia C: 192.168.16.254/24)



Dopo aver assegnato gli indirizzi IP ai vari PC delle reti e alle interfacce dei router, e aver configurato i router (come nella lezione precedente), andiamo a configurare il ◀ server FTP ▶.

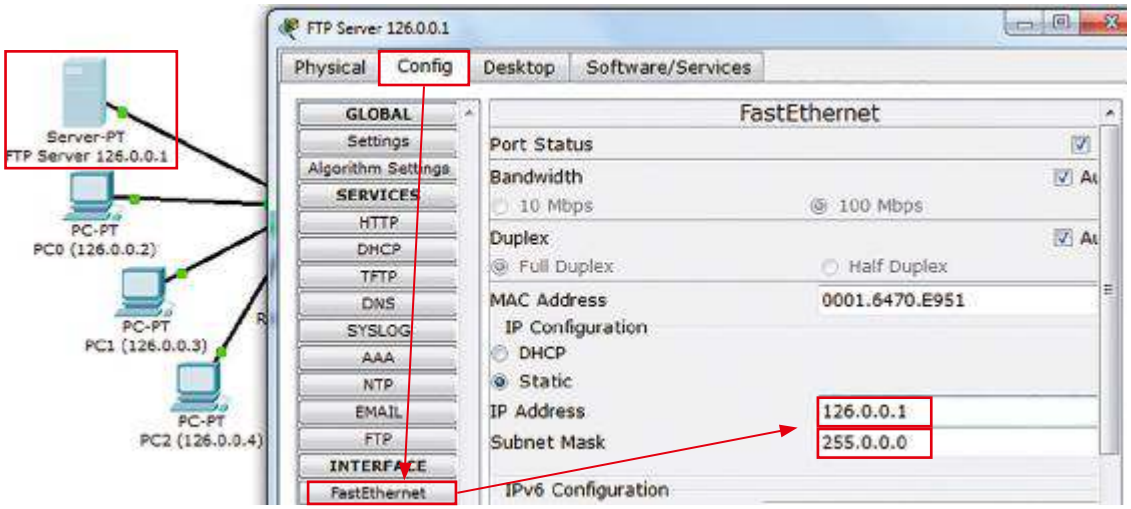
◀ Un server FTP è un'applicazione gestita da un amministratore di sistema o da un provider di servizi Internet (ISP), e responsabile della gestione delle richieste provenienti dal client FTP di un utente. I comandi inviati al server FTP, così come le risposte ottenute dal server stesso, vengono trasferite in formato ASCII. ▶

Sia il protocollo FTP che il protocollo HTTP consentono il trasferimento dei file utilizzando il protocollo TCP per il trasporto degli stessi. Il protocollo FTP viene anche definito protocollo con controllo fuori banda e utilizza due connessioni TCP parallele:

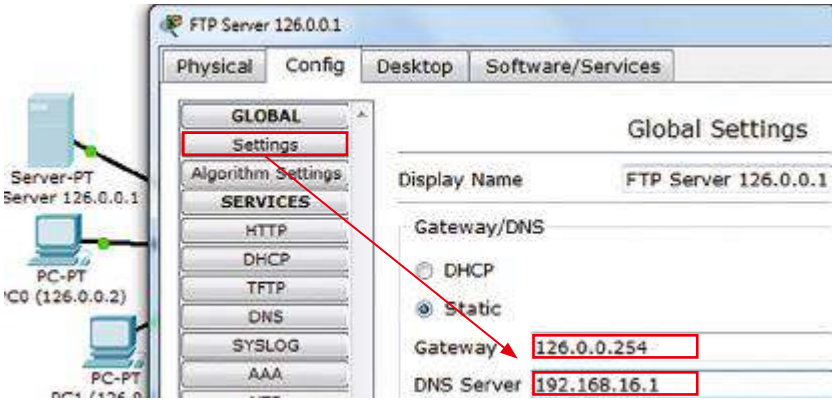
- connessione di controllo, veicola informazioni di controllo del protocollo (identificazione e comandi);
- connessione dati, per il trasferimento dati vero e proprio.

Il protocollo HTTP invece spedisce le informazioni di controllo nella stessa connessione usata per i dati, per questo viene infatti definito con controllo in banda.

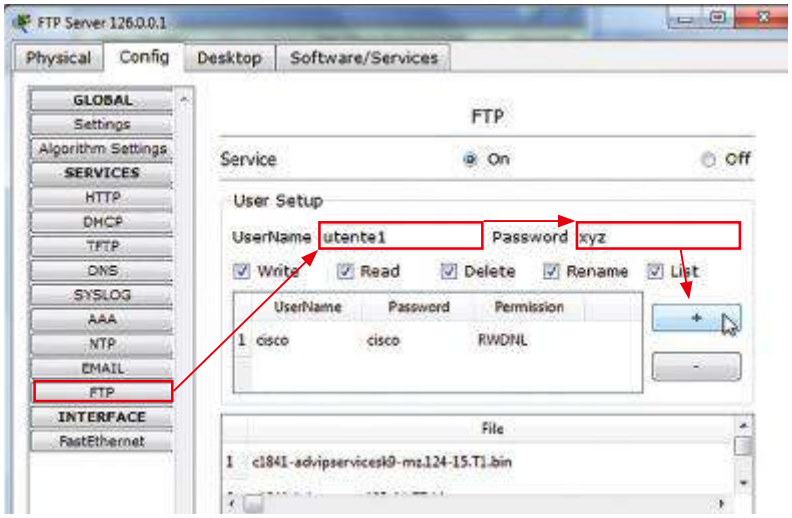
1. Vediamo innanzi tutto di configurare gli indirizzi del server FTP, facendo clic sull'icona del server, quindi Config, poi clicchiamo su FastEthernet e scriviamo l'indirizzo di rete del server (126.0.0.1) e la maschera di rete (255.0.0.0) nelle caselle relative:



2. Sempre nella scheda Config del server FTP, facciamo clic su Settings e andiamo a definire l'indirizzo di Gateway (126.0.0.254) e del DNS server (192.168.1.1):



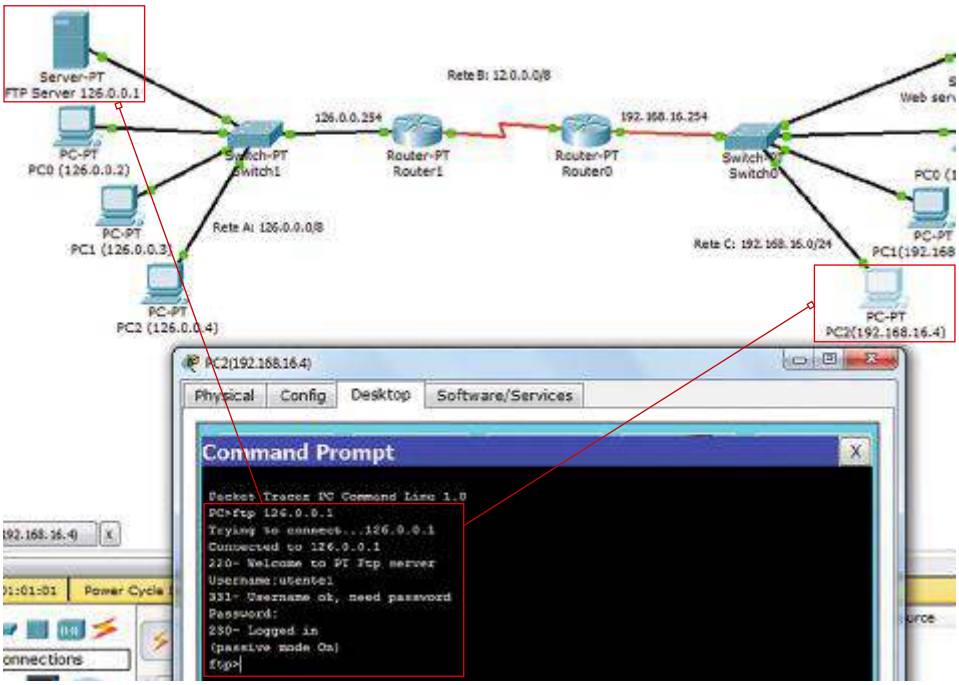
3. Passiamo adesso alla configurazione del servizio FTP sul server, facendo clic su FTP nella scheda Config. Verifichiamo che il servizio FTP (Service) sia su On, quindi passiamo ad aggiungere un nuovo utente con i tutti permessi attivati (RWDNL), cioè Write, Read, Delete, Rename, List. Facciamo clic sul pulsante "+" per aggiungere effettivamente l'utente all'elenco:



L'utente cisco, con password cisco è presente di default nell'elenco degli utenti. Come possiamo vedere possiede anch'esso i permessi di amministratore, cioè Scrittura, Lettura, Cancellazione, Modifica dei nomi e Lista. Inoltre nella sezione denominata File sono presenti alcuni file, a titolo di prova, utili per eseguire i comandi FTP necessari a testare il funzionamento del server.

Connessione remota al server FTP

1. Vediamo come effettuare la connessione remota da un PC all'FTP server. Scegliamo di connetterci dal PC2 della rete C, per fare questo facciamo clic sul PC2, quindi scegliamo Desktop, poi Command Prompt. All'interno del Command Prompt possiamo digitare i comandi FTP necessari alla connessione, in questo caso digitiamo il comando `ftp` seguito dall'indirizzo IP del server, in questo caso `126.0.0.1`.



2. Dopo aver inserito il nome dell'utente e la password, viene mostrato il prompt ftp> che segnala l'avvenuta connessione e segnala che l'utente può incominciare a impartire i comandi per il trasferimento di file.

Zoom su...

COMANDI FTP

ftp *hostname*: apre la connessione all'indirizzo indicato da hostname;
cd *nuova_direcory*: cambia la directory remota corrente;
pwd: visualizza la directory remota corrente;
dir: mostra l'elenco dei file e delle sottodirectory della directory remota corrente;
help *nome_comando*: visualizza i comandi supportati da FTP;
put *nome_file*: invia un file dalla stazione locale alla stazione remota;
get *nome_file*: riceve un file dalla stazione remota sulla stazione locale.

3 Digitiamo il comando `dir` per ottenere la lista dei file presenti sul server.

```
ftp>dir

Listing /ftp directory from 126.0.0.1:
0    : c1841-advipservicesk9-mz.124-15.T1.bin          33591768
1    : c1841-ipbase-mz.123-14.T7.bin                   13832032
2    : c1841-ipbasek9-mz.124-12.bin                    16599160
3    : c2600-advipservicesk9-mz.124-15.T1.bin          33591768
4    : c2600-i-mz.122-28.bin                           5571584
5    : c2600-ipbasek9-mz.124-8.bin                     13169700
6    : c2800nm-advipservicesk9-mz.124-15.T1.bin        50938004
7    : c2800nm-ipbase-mz.123-14.T7.bin                 5571584
8    : c2800nm-ipbasek9-mz.124-8.bin                   15522644
9    : c2950-i6q412-mz.121-22.EA4.bin                  3058048
10   : c2950-i6q412-mz.121-22.EA8.bin                  3117390
11   : c2960-lanbase-mz.122-25.FX.bin                  4414921
12   : c2960-lanbase-mz.122-25.SEE1.bin                4670455
13   : c3560-advipservicesk9-mz.122-37.SE1.bin         8662192
14   : pt1000-i-mz.122-28.bin                          5571584
15   : pt3000-i6q412-mz.121-22.EA4.bin                 3117390
ftp>
```

4 Dopo aver individuato il file numero 4 dell'elenco visto sopra, passiamo a effettuarne il download mediante il comando `get`, seguito dal nome del file da scaricare:

```
ftp>get c2600-i-mz.122-28.bin

Reading file c2600-i-mz.122-28.bin from 126.0.0.1:
File transfer in progress...

[Transfer complete - 5571584 bytes]

5571584 bytes copied in 14.325 secs (89118 bytes/sec)
ftp>
```

5 Verifichiamo di aver effettivamente scaricato il file. Per fare questo chiudiamo e riapriamo la finestra `Command Prompt`, quindi digitiamo il comando dir per ottenere la lista dei file memorizzati sul client. Come possiamo notare il file scaricato in precedenza è adesso presente sul PC:

```
PC>dir

 Volume in drive C has no label.
 Volume Serial Number is 5E12-4AF3
 Directory of C:\
  1/1/1970    1:0 PM        5571584            c2600-i-mz.122-28.bin
  2/7/2106    7:28 PM       26                 sampleFile.txt
                            5571610 bytes      2 File(s)
PC>
```

6 Proviamo adesso a caricare un file sul server: per fare questo utilizziamo il comando put, seguito dal nome del file, in questo caso rappresentato dal file sampleFile.txt:

```
ftp>put sampleFile.txt

Writing file sampleFile.txt to 126.0.0.1:
File transfer in progress...

[Transfer complete - 26 bytes]

26 bytes copied in 0.056 secs (464 bytes/sec)
ftp>
```

7 Per verificare l'avvenuto upload del file digitiamo il comando dir: possiamo individuare il file sampleFile.txt nell'elenco che appare.

```
ftp>dir

Listing /ftp directory from 126.0.0.1:
0   : c1841-advipservicesk9-mz.124-15.T1.bin          33591768
1   : c1841-ipbase-mz.123-14.T7.bin                   13832032
2   : c1841-ipbasek9-mz.124-12.bin                    16599160
3   : c2600-advipservicesk9-mz.124-15.T1.bin          33591768
4   : c2600-i-mz.122-28.bin                           5571584
5   : c2600-ipbasek9-mz.124-8.bin                     13169700
6   : c2800nm-advipservicesk9-mz.124-15.T1.bin        50938004
7   : c2800nm-ipbase-mz.123-14.T7.bin                 5571584
8   : c2800nm-ipbasek9-mz.124-8.bin                   15522644
9   : c2950-i6q412-mz.121-22.EA4.bin                  3058048
10  : c2950-i6q412-mz.121-22.EA8.bin                  3117390
11  : c2960-lanbase-mz.122-25.FX.bin                  4414921
12  : c2960-lanbase-mz.122-25.SEE1.bin                4670455
13  : c3560-advipservicesk9-mz.122-37.SE1.bin         8662192
14  : pt1000-i-mz.122-28.bin                          5571584
15  : pt3000-i6q412-mz.121-22.EA4.bin                 3117390
16  : sampleFile.txt                                  26
```

Prova adesso!

• Applicare un server FTP

APRI IL FILE DNS_FTP.pkt

1 Modifica l'esempio aggiungendo un altro FTP server nella rete C e configurandolo con l'aggiunta del servizio FTP.

2 Dopo aver aggiunto alcuni utenti, verifica la connessione tra server e client, caricando il file sampleFile.txt e scaricando dal server alcuni file a piacere.

Esercitazioni di Laboratorio 4

HTTP SNIFFING CON WIRESHARK

Scopo di questa esercitazione è quello di catturare due pacchetti e analizzarli individuando le caratteristiche del protocollo HTTP utilizzano il packet-sniffer Wireshark.

> Il pacchetto Wireshark è stato descritto nell'esercitazione di laboratorio Utilizzo di Wireshark del volume 1, che è anche reperibile tra le risorse on-line del presente volume sul sito www.hoepliscuola.it.

Generalità del protocollo HTTP

È il protocollo fondamentale del World Wide Web (WWW) descritto nella RFC 1945 (versione HTTP/1.0) nelle RFC 2068 e RFC 2616 (versione HTTP/1.1).
Ha la caratteristica di essere un protocollo client-server completamente testuale che utilizza la porta 80: è di tipo Stateless ma il server può implementare tecniche per mantenere lo stato quali i cookies, le sessioni, campi nascosti nei form, URL re direction ecc.

Il client invia una richiesta contenente un metodo al server, composta da tre parti:
- riga di richiesta (*request line*);
- intestazione (*header*);
- corpo del messaggio(*body*) (*opzionale*).

Nella riga di richiesta si trovano i metodi HTTP, come GET, POST, HEAD, PUT, DELETE ecc.

Gli header forniscono informazioni sul contenuto della richiesta e hanno il seguente formato:

Header: valore →

From: adamo@paradiso.it
Host: www.eden.it
User-Agent: Mozilla/5.0
Accept-Language: en-us, it-it
Keepalive: 300
Accept: text/xml

> Se un messaggio HTTP contiene un **body**, a seguito dell'header devono essere specificate le proprietà nell'header stesso.

A seguito della richiesta il server invia una risposta che ha una struttura analoga a quella della domanda: la riga di richiesta prende il nome di status line e i messaggi sono codificati con numeri di tre cifre dove la cifra delle centinaia li raggruppa come riportato nella tabella seguente:

Codice	Significato
1xx:	informazione
2xx:	successo
3xx:	redirezione (la richiesta è corretta ma è stata rediretta a un altro server)
4xx:	errore lato client (richiesta errata)
5xx:	errore lato server (c'è un problema interno del server)

Al codice segue sempre un messaggio di testo, generalmente in lingua inglese, che aiuta l'utente alla comprensione della risposta.

Zoom su...

STATUS CODE

Di seguito è riportato a titolo di esempio un elenco parziale di status code definiti nell'RFC 2616: l'elenco completo è reperibile all'indirizzo http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html.

- 301 Moved Permanently: la risorsa è stata spostata in un'altra locazione in maniera permanente;
- 304 Not Modified: la risorsa non è stata modificata dall'ultima volta, non serve rinviarla;
- 400 Bad Request: il server non è in grado di capire la richiesta;
- 404 Not Found: la risorsa richiesta non è disponibile (per esempio, è stata richiesta una pagina inesistente);
- 500 Internal server Error: c'è stato un errore interno nel server (per esempio, un errore di connessione al db).

Alla status line fa seguito un insieme di header e un body che contiene la risposta, che sono i contenuti della richiesta al server (pagina HTML, immagini, filmati ecc.).

L'interazione di base: richiesta/risposta

Come prima parte di esercitazione sul protocollo HTTP scarichiamo alcuni file da un dominio Web, catturiamo con Wireshark i pacchetti che vengono scambiati tra il nostro host e il server e li analizziamo sempre con Wireshark.

Se non avete la possibilità di catturare i pacchetti potete analizzare quelli disponibili tra le risorse online nella sezione dedicata a questo libro nel sito www.hoepliscuola.it, nella cartella risorse, memorizzati nei file HTTP-file1.pcap e HTTP-file2.pcap.

Iniziamo a esplorare il protocollo HTTP scaricando un semplice file HTML molto piccolo, che non contiene nessun altro oggetto o contenuto multimediale (immagine, suono ecc.).

1. Manda in esecuzione Wireshark e setta come filtro HTTP, come in figura ▶:

2. Utilizzando il tuo browser connetteti a Internet alla pagina

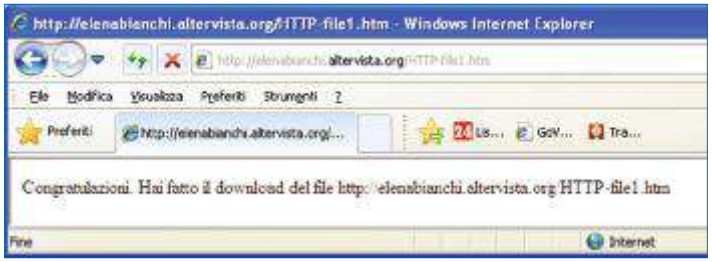
   http://elenabianchi.altervista.org/HTTP-file1.htm

   oppure alla pagina

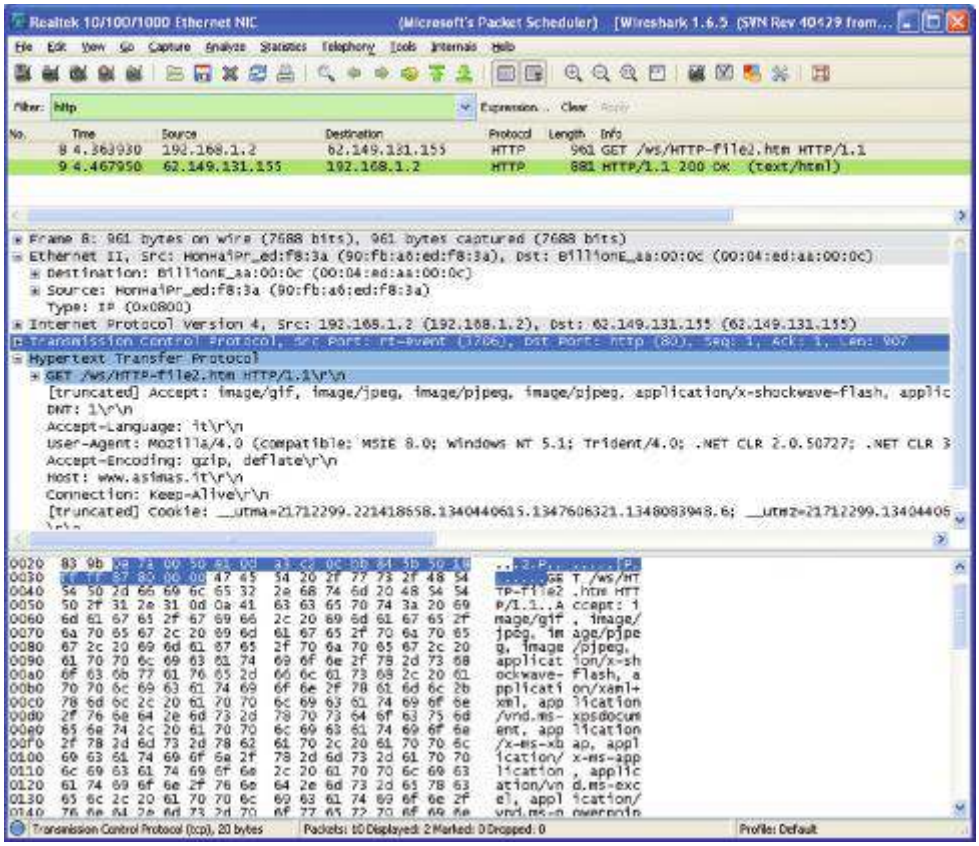
   http://www.hoepliscuola.it//media/File/esercizi/5025-3/es01/HTTP-file1.htm

   In questo modo nella finestra dell'elenco dei pacchetti vengono visualizzati solo i pacchetti contenenti messaggi HTTP.

3. Nel browser viene visualizzata una pagina HTML con una sola riga, come indicato nella figura: ▶



4. Interrompi la cattura dei pacchetti: la finestra di Wireshark dovrebbe essere simile a quella riportata di seguito.



Sono presenti due messaggi HTTP: il messaggio GET, che ha inviato la richiesta dal vostro browser al server, e il messaggio di risposta verso il vostro browser.
La finestra centrale, quella di dettaglio, mostra informazioni del messaggio selezionato (nel caso di figura il primo): sono presenti le informazioni dell'intero frame Ethernet, dato che il messaggio HTTP è trasportato all'interno di un segmento TCP che a sua volta è all'interno di un datagramma IP, che è contenuto nel frame Ethernet.
Per espandere solo i dati che ci interessa analizzare basta cliccare sui box a fianco delle righe settando con [+] la riga desiderata e [-] quelle che si vogliono compattare.

Nella finestra potrebbero anche essere presenti messaggi relativi al file favicon.ico: con questo messaggio HTTP GET il vostro browser potrebbe chiedere automaticamente di visualizzare la piccola icona che viene visualizzata alla sinistra della riga di indirizzo della finestra del browser.

Prova adesso!

Rispondi alle seguenti domande, stampando i messaggi corrispondenti per meglio indicare le risposte:

1. Quale versione di HTTP sta usando il tuo browser?
2. Quale versione di HTTP è in esecuzione sul server?
3. Il tuo browser è in grado di accettare e, quindi, di interpretare qualche linguaggio?
4. Qual è l'indirizzo IP del tuo computer?
5. Qual è l'indirizzo IP del server?
6. Qual è il codice di stato restituito dal server al tuo browser?
7. Quando è stato modificato l'ultima volta il file che hai recuperato dal server?
8. Se individui che il file è stato modificato qualche minuto prima del tuo download, prova a riscaricarlo e confronta nuovamente l'ora dell'ultima modifica. Cosa puoi osservare? Perché?
9. Quanti byte sono stati inviati al tuo browser?

Il server e il browser continuano a scambiarsi messaggi: Wireshark li intercetta ed è possibile visualizzarli cliccando col tasto destro su uno qualunque dei pacchetti che fanno parte della connessione TCP e selezionare Follow TCP Stream.

Recuperare documenti di grandi dimensioni

Come secondo esercizio ci proponiamo ora di analizzare il protocollo HTTP mentre scarichiamo un file di dimensioni abbastanza grandi da richiedere più invii.

La maggior parte dei browser mantiene una cache con gli ultimi oggetti scaricati: prima di eseguire il prossimo esercizio assicuratevi che la cache del vostro browser sia vuota
- per IE, selezionate Strumenti → Elimina cronologia esplorazione → Elimina.
- per Firefox, selezionate Strumenti → Cancella cronologia recente → Cancella adesso.

1. Avvia il browser Web e svuota la cache.

2. Manda in esecuzione Wireshark.

3. Immetti la seguente URL nel browser:

   http://elenabianchi.altervista.org/HTTP-file2.htm

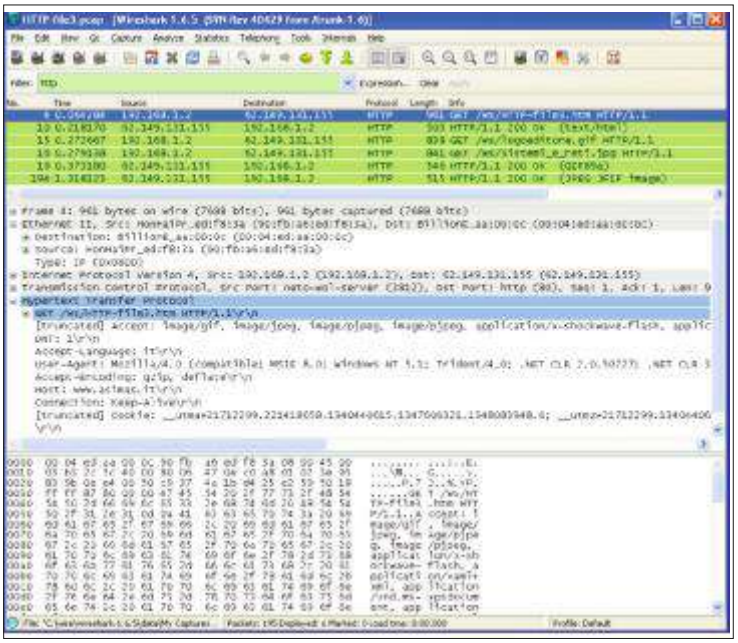
   oppure il seguente indirizzo

   http://www.hoepliscuola.it//media/File/esercizi/5025-3/es01/HTTP-file2.htm

4. Il tuo browser visualizza la seguente pagina contenente due immagini. ▶

5. Interrompi la cattura pacchetti di Wireshark.

6. Filtra i messaggi inserendo come nell'esercizio precedente "HTTP" nella finestra del filtro: si ottiene una situazione simile a quella riportata nella figura. ▶



Nella finestra sono ora presenti più righe: seleziona la risposta alla prima GET (seconda riga) e osserva nella finestra dei dettagli quelli relativi al protocollo HTTP individuando la riga denominata "Reassembled TCP Segments".

Il protocollo TCP ha spezzato il file richiesto in più parti, dato che la sua dimensione è di circa 4 Kbyte e quindi è superiore al valore massimo per MTU di 1500 byte imposti da Ethernet: la risposta viene quindi frammentata in alcuni pacchetti tra loro separati dove il primo contiene la dicitura "Reassembled TCP Segments" per indicare che sarà seguito dai rimanenti pacchetti che formano l'intero messaggio HTTP.

Prova adesso!

Rispondi alle seguenti domande, stampando i messaggi corrispondenti per meglio indicare le risposte:

1. Quanti messaggi HTTP GET sono stati inviati dal vostro browser?
2. A quali indirizzi Internet sono state inviate queste richieste?
3. Quanti segmenti contenenti dati sono stati necessari per trasportare l'unica risposta HTTP?
4. Qual è la dimensione di ogni singolo segmento?
5. Qual è il codice di stato e la frase associata alla risposta del server?
6. Ci sono righe di stato HTTP trasmesse nei pacchetti TCP di risposta successivi al primo?
7. Come sono state scaricate le due immagini dal vostro browser?
8. Come si riesce a comprendere che appartengono alla pagina da voi richiesta?

Esercizi proposti

1. Prova a ottenere dal Web server un messaggio di risposta con la Status Line 400 Bad Request.
2. Prova a ottenere dal Web server un messaggio di risposta con la Status Line 404 Not Found.
3. Scarica dal Web un file immagine di dimensione superiore a 20 Kbyte e analizzane il pacchetti.
4. Collegati a un sito che richiede una autenticazione e cerca di individuare, analizzando i pacchetti scambiati tra client e server, i dati di autenticazione (user name e password).

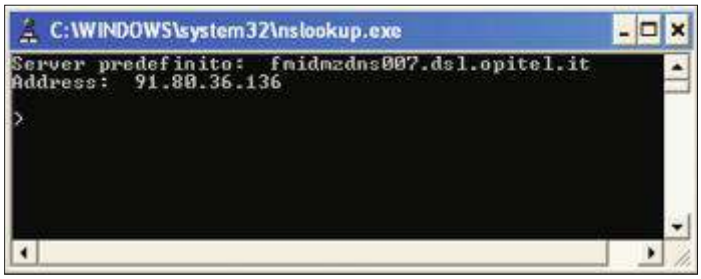
Esercitazioni di Laboratorio 5

DNS E NSLOOKUP

Il Domain Name System (DNS), come descritto nella lezione 6, traduce nomi di host in indirizzi IP, e in questa esercitazione analizzeremo cosa avviene alla richiesta di un client di risoluzione di un indirizzo: sappiamo che i server DNS gerarchici comunicano tra di loro ricorsivamente o iterativamente per rispondere alla query, in modo del tutto trasparente al client che ha posto la domanda.

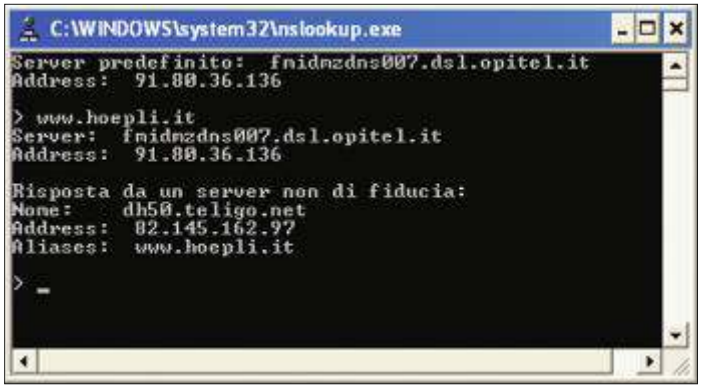
Il programma Nslookup

I sistemi operativi Linux/Unix e Microsoft mettono a disposizione il comando nslookup che ci permette di inviare una query DNS al server DNS specificato e di visualizzare la risposta ricevuta.
Basta posizionarsi sulla linea di comando e digitare nslookup per visualizzare la seguente schermata:



Per uscire e terminare l'interrogazione si digita il comando EXIT.

Come si può vedere nella seguente videata, è possibile interrogare sia un server radice, un server di dominio top-level, un server di fiducia (authoritative) oppure un server DNS intermedio.



Il comando può anche essere eseguito con l'opzione type=NS: in questo caso viene richiesto di specificare i server di competenza (authoritative) per il dominio ricercato.

In questo esempio il client è localizzato a Milano e il server DNS locale è fmidmzdns007.dsl.opitel.it.

Prova adesso!

Spesso i firewall presenti nella rete delle aule di informatica non permettono di interrogare un server DNS a scelta ma solo quello locale, mentre dal "PC casalingo" è possibile effettuare tutte le interrogazioni.

Rispondi alle seguenti domande, stampando i messaggi corrispondenti per meglio indicare le risposte:

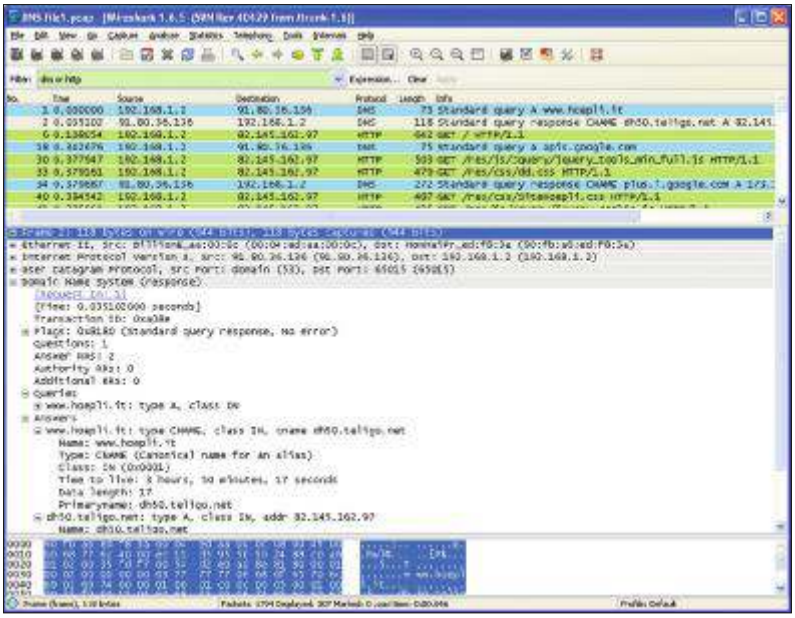
1. Quanti messaggi HTTP GET sono stati inviati dal tuo browser?
2. A quali indirizzi Internet sono state inviate queste richieste?
3. Quanti segmenti contenenti dati sono stati necessari per trasportare l'unica risposta HTTP?
4. Qual è la dimensione di ogni singolo segmento?
5. Qual è il codice di stato e la frase associata alla risposta del server?
6. Ci sono righe di stato HTTP trasmesse nei pacchetti TCP di risposta successivi al primo?
7. Come sono state scaricate le due immagini dal tuo browser?
8. Come si riesce a comprendere che appartengono alla pagina da te richiesta?

Tracciare il protocollo DNS con Wireshark

Cattura ora i pacchetti che vengono scambiati con Wireshark.

1. Apri il browser e, per precauzione, svuota la cache.
2. Manda in esecuzione Wireshark e immetti "dns or http" nel filtro (in minuscolo) per visualizzare solo i pacchetti relativi ai protocolli DNS e HTTP.
3. Inizia a effettuare la cattura dei pacchetti con Wireshark.
4. Visita la pagina Web http://www.hoepli.it.
5. Interrompi la cattura dei pacchetti.

Ripeti ora le operazioni per la cattura dei pacchetti:



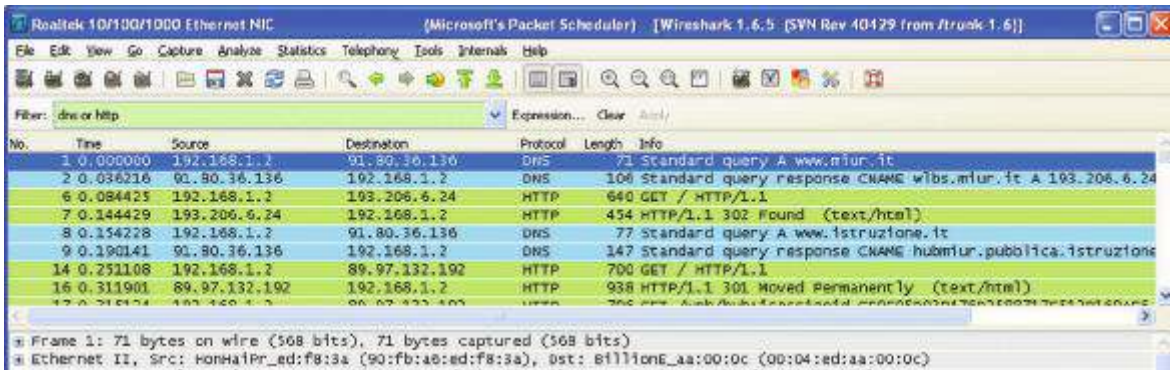
Prova adesso!

Rispondi alle seguenti domande.

1. Le query DNS e i messaggi di risposta con che protocollo sono inviati?
2. Qual è la porta di destinazione per le query DNS?
3. Qual è la porta sorgente per i messaggi DNS di risposta?
4. Individua l'indirizzo IP del tuo server DNS locale mediante il comando ipconfig.
5. Individua a quale indirizzo IP è stata mandata la query DNS.
6. Confronta i due indirizzi e commenta il risultato.
7. Individua il "Type" della query DNS.
8. Individua la risposta DNS: cosa contengono i record di risposta?
9. Questa pagina Web contiene immagini. Prima di recuperare queste immagini, sono state inviate altre query DNS?

1. Apri il tuo browser e, per precauzione, svuota la cache.
2. Manda in esecuzione Wireshark e immetti "dns or http" nel filtro (in minuscolo) per visualizzare solo i pacchetti relativi ai protocolli DNS e HTTP.
3. Inizia a effettuare la cattura dei pacchetti con Wireshark.
4. Visita la pagina Web http://www.MIUR.it.
5. Interrompi la cattura dei pacchetti.

Dovresti ottenere una videata simile alla seguente:



Prova adesso!

Rispondi quindi alle seguenti domande.

1. Quante query sono state inviate?
2. Individua la porta di destinazione per il messaggio DNS di richiesta.
3. Individua la porta di destinazione per il messaggio DNS della risposta.
4. La richiesta DNS è stata mandata al tuo DNS locale? Scrivi l'indirizzo.
5. Individua il "Type" della query DNS.
6. Individua la risposta DNS: cosa contengono i record di risposta?

Esercitazioni di Laboratorio 6

SMTP E POP: SNIFFING CON WIRESHARK

Generalità sul Simple Mail Transfer Protocol (SMTP)

Il Simple Mail Transfer Protocol (SMTP) è il protocollo standard per la trasmissione di email via Internet. È un protocollo client/server relativamente semplice, testuale, nel quale vengono specificati uno o più destinatari di un messaggio e, verificata la loro esistenza, il messaggio viene trasferito.
Il protocollo SMTP usa il protocollo di trasmissione TCP e, per accedervi, la porta 25: per l'invio della posta elettronica è necessario avere installato un software client come Opera 10, Mozilla Thunderbird, Outlook Express, The Email Client, Eudora ecc.
Sendmail fu uno dei primi (se non proprio il primo) programma a implementare il protocollo SMTP: fino a oggi sono stati scritti oltre 100 programmi che implementano il protocollo SMTP come client (mittente dei messaggi) o server (destinatario del messaggio).

Non basta avere istallato il software per spedire la posta in quanto è necessario poter accedere al server SMTP che inoltrerà i nostri messaggi al destinatario: i fornitori di connettività provvedono a fornire i parametri e le credenziali per poter effettuare l'autenticazione al server SMTP in modo da permettere ai propri clienti di inviare posta elettronica attraverso i programmi client, ma solo mediante un indirizzo connesso al proprio dominio. Nella figura è riportata la scheda di configurazione del gestore di telefonia TeleTu.

La posta spedita viene memorizzata nel server che provvede a effettuare la consegna al server che gestisce la casella di posta (mailbox) del/dei destinatario/i.
Poiché SMTP è un protocollo testuale basato sulla codifica ASCII, non è permesso trasmettere direttamente testo composto con un diverso set di caratteri e tantomeno file binari: a tale scopo si utilizza lo standard MIME, che permette di estendere il formato dei messaggi mantenendo la compatibilità col software esistente.

L'SMTP è un protocollo che permette soltanto di inviare messaggi di posta, ma non di richiederli a un server: per fare questo il client di posta deve usare altri protocolli, quali il POP3 (Post Office Protocol) e l'IMAP (Internet Message Access Protocol).

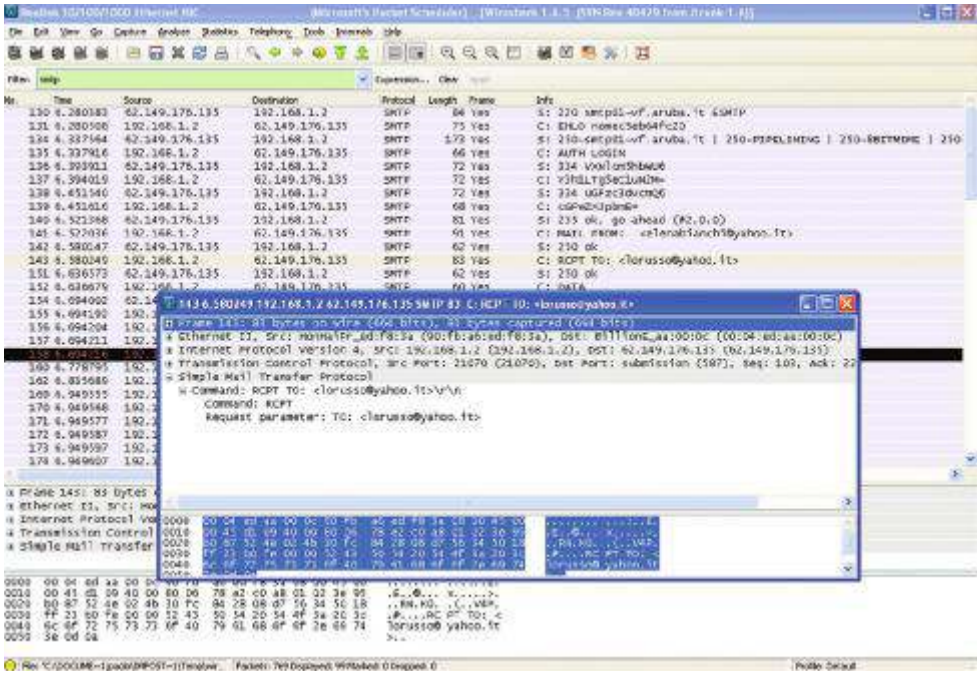
Cattura di pacchetti SMTP

Per poter verificare il corretto invio del messaggio email è necessario possedere un indirizzo email reale al quale poter accedere per visionare il messaggio di posta inviato.

Per poter capire il funzionamento del protocollo SMTP si effettuerà un invio di email utilizzando un client dedicato: spesso i laboratori scolastici non permettono di effettuare questa attività e quindi si consiglia di effettuare questa esercitazione sul PC domestico e di salvare i pacchetti per poi analizzarli successivamente in laboratorio.

1. Avvia un client di posta elettronica e prepara un messaggio: si consiglia di inviare un messaggio email a un proprio account esistente e attivo, dal quale si possa poi, tramite webmail, controllarne l'avvenuta ricezione.
2. Avvia Wireshark e inizia a effettuare la cattura dei pacchetti.
3. Invia il messaggio di posta.
4. Termina la cattura e salva i pacchetti che sono stati intercettati in un file (per esempio, salva i pacchetti in smtp1.pcap).
5. Filtra i pacchetti ricevuti inserendo smtp (in minuscolo) nella linea Filter.

A video si presenta una schermata come quella riportata di seguito:



Prova adesso!

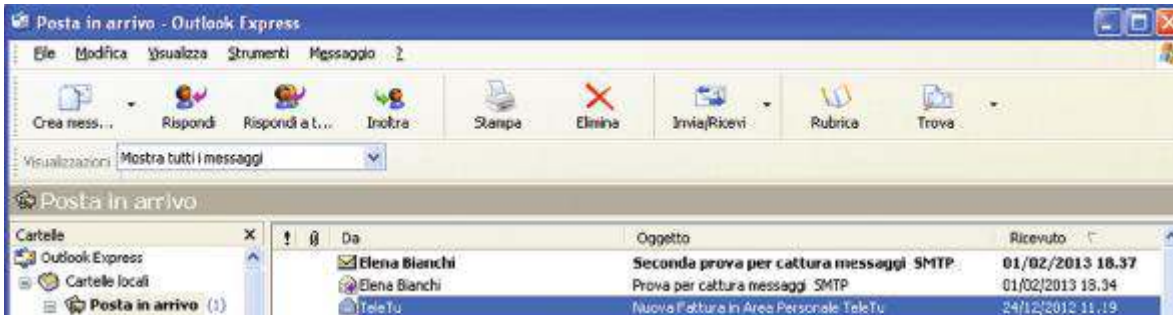
1. Individua le righe dove avviene la autenticazione da parte del server: cosa si può osservare?
2. Qual è il significato del codice 220 inviato dal server al client?
3. Evidenzia il mittente e il destinatario del messaggio.
4. Qual è il server di posta in uscita? Dove è possibile individuarlo?
5. Quali sono le dimensioni del messaggio inviato?
6. Individua il pacchetto che contiene l'oggetto del messaggio.
7. Cosa si può osservare in merito alla privacy?
8. Ora ripeti le operazioni di invio componendo un nuovo messaggio che comprende un allegato (per esempio, una immagine con dimensioni maggiori di 10 Kbyte).
9. Come varia il traffico catturato con Wireshark?
10. Come viene gestito l'invio dell'allegato?

Il Post Office Protocol (POP)

Il Post Office Protocol è un protocollo che permette alle persone autenticate di accedere a un account di posta elettronica presente su di un host per scaricare le email del relativo account utilizzando un software di posta (come per esempio Outlook Express).
Come per l'invio dei parametri per la lettura della posta sono forniti dal server che offre il sevizio e vengono inseriti nella configurazione dell'account del destinatario della posta: la ricezione dei messaggi sul PC locale è generalmente permessa da tutti i gestori del servizio di comunicazione, anche per account registrate su altri domini.

> Il protocollo POP3 non prevede alcun tipo di cifratura, quindi le password utilizzate per l'autenticazione fra server e client passano in chiaro: l'evoluzione del protocollo POP che utilizza MD5 è APOP.

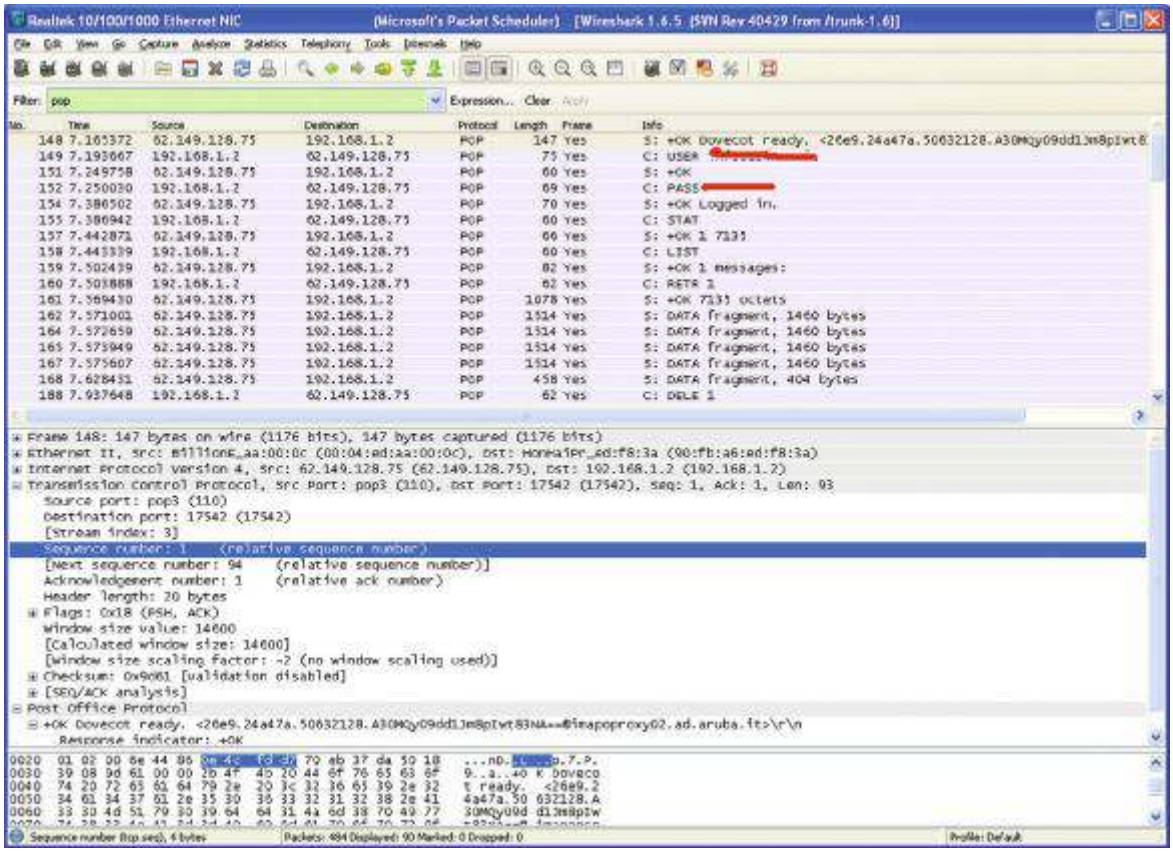
1. Manda in esecuzione Wireshark in modo da catturare i pacchetti.
2. Avvia il client di posta elettronica per esempio, Outlook express.
3. Quando la posta è scaricata, ferma Wireshark: dovresti ricevere "almeno" i due messaggi prima spediti durante l'esercizio sul SMTP.



4. Termina la cattura e salva i pacchetti che sono stati intercettati in un file (per esempio, salva i pacchetti in smtp2.pcap).

5. Filtra i pacchetti ricevuti inserendo pop (in minuscolo) nella linea Filter.

A video dovresti avere una situazione simile a quella di figura:



È anche possibile isolare i messaggi usando un filtro con l'indirizzo IP: nel nostro esempio inserendo

ip.addr==192.168.1.2 // indirizzo del mittente

oppure

ip.addr==62.149.128.75 // indirizzo destinatario

Se dalla rete scolastica fosse impossibile effettuare l'esecuzione di un programma client di posta elettronica puoi scaricare il file smtp2.pcap dalla cartella materiali dello spazio Web riservato a questo volume all'indirizzo www.hoepliscuola.it

Prova adesso!

1. Individua le righe dove avviene la autenticazione da parte del server: cosa si può osservare?
2. A che porta del server il client si è connesso per ricevere il messaggio?
3. Evidenzia il mittente e il destinatario del messaggio.
4. Dove è possibile individuare il server di posta?
5. Quali sono le dimensioni del messaggio inviato?
6. Individua il pacchetto che contiene l'oggetto del messaggio.
7. Ora ripeti le operazioni analizzando i pacchetti ricevuti per il secondo messaggio, quello contenente l'allegato.
8. Come varia il traffico catturato con Wireshark?
9. Come viene gestita la ricezione dell'allegato?
10. Che tipo di encoding è usato per l'allegato?
11. Quanti bit vengono usati per l'encoding?

CLIL

Application layer

The Application Layer can include things like File Transfers, and display formatting. HTTP is an example of an Application Layer protocol. Commonly known protocols considered by many to be part of the Application Layer may actually be considered to occupy the Session, Presentation, and Application Layers. For example, an examination of an NFS file mount with files being copied defies simple categorization within the ISO OSI 7 Layer Reference Model. Is NFS an Application Layer Protocol? Well, files are copied, so we see that the Application Layer may be included. However, synchronization in file transfers takes place to some extent and session are created and torn down on demand as files are transferred. This suggests that it could also be part of the session layer or maybe presentation layer.

Level 7

In the Open Systems Interconnection (OSI) communications model, Level 7 provides services for an application program to ensure that effective communication with another application program in a network is possible. Level 7 is not the application itself that is doing the communication. It is a service level that provides these services:

- Makes sure that the other party is identified and can be reached.
- If appropriate, authenticates either the message sender or receiver or both.
- Makes sure that necessary communication resources exist (for example, is there a modem in the sender's computer?).
- Ensures agreement at both ends about error recovery procedures, data integrity, and privacy.
- Determines protocol and data syntax rules at the application level.

DNS (Domain Name System)

Short for Domain Name System (or Service or Server), an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet, however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4.

The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

FTP (File Transfer Protocol)

FTP is a standard network protocol used to transfer files from one computer to another computer over a TCP-based network, such as the Internet. FTP is often used to upload web pages and other documents from a private development machine to a public web-hosting server. A network protocol is simply a standard language that allows computers to communicate. So FTP is a way for computers to communicate like we use English to communicate among ourselves. File Transfer Protocol is how you transfer files using a common computer language.

HTTP Request and Response Header

The HTTP Request header is the information, in the form of a text record, that a user's browser sends to a Web server containing the details of what the browser wants and will accept back from the server. The request header also contains the type, version and capabilities of the browser that is making the request so that server returns compatible data. Upon receipt of the request header, the server will return an HTTP response header to the client that is attached to the file(s) being sent. The HTTP Response header is the information, in the form of a text record, that a Web server sends back to a client's browser in response to receiving an HTTP request. The response header contains the date, size and type of file that the server is sending back to the client and also data about the server itself. The header is attached to the files being sent back to the client.

FTP Server

File Transfer Protocol (FTP) is the commonly used protocol for exchanging files over the Internet. FTP uses the Internet's TCP/IP protocols to enable data transfer. FTP uses a client-server architecture, often secured with SSL/TLS. FTP promotes sharing of files via remote computers with reliable and efficient data transfer. FTP works in the same way as HTTP for transferring Web pages from a server to a user's browser and SMTP for transferring electronic mail across the Internet in that, like these technologies, FTP uses a client-server architecture. Users provide authentication using a sign-in protocol, usually a username and password, however some FTP servers may be configured to accept anonymous FTP logins where you don't need to identify yourself before accessing files. Most often, FTP is secured with SSL/TLS.

Files can be transferred between two computers using FTP software. The user's computer is called the local host machine and is connected to the

Internet. The second machine, called the remote host, is also running FTP software and connected to the Internet.

- The local host machine connects to the remote host's IP address.
- The user would enter a username/password (or use anonymous).
- FTP software may have a GUI, allowing users to drag and drop files between the remote and local host. If not, a series of FTP commands are used to log in to the remote host and transfer files between the machines.

SMTP Server

Short for Simple Mail Transfer Protocol, a protocol for sending e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP or IMAP. In addition, SMTP is generally used to send messages from a mail client to a mail server. This is why you need to specify both the POP or IMAP server and the SMTP server when you configure your e-mail application.

Telnet

Telnet is a terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers. The Telnet protocol is designed to provide a bi-directional, eight-bit byte oriented communications facility to allow for a standard method of interfacing terminal devices and processes.

UNITÀ DI APPRENDIMENTO

2

VLAN: Virtual Local Area Network

L1 **Le Virtual LAN (VLAN)**
L2 **Il protocollo VTP e l'Inter VLAN-Routing**

Esercitazioni di laboratorio

1 Realizziamo una VLAN con Packet Tracer; 2 I comandi CLI per configurare la VLAN; 3 VLAN e VTP con Packet Tracer

Conoscenze

- Conoscere le caratteristiche delle VLAN
- Individuare pregi e difetti delle VLAN
- Acquisire le caratteristiche delle VLAN port based
- Riconoscere VLAN tagged, untagged e ibride
- Conoscere il protocollo VTP
- Conoscere l'Inter-VLAN routing

Competenze

- Applicare le VLAN in base alla tipologia di rete richiesta
- Configurare VLAN anche in presenza di più switch

Abilità

- Configurare gli switch singolarmente
- Saper configurare le VLAN
- Utilizzare il protocollo VTP per definire le VLAN

AREA digitale

Esercizi

Soluzioni
Puoi scaricare il file anche da hoepliscuola.it

LEZIONE 1

Le Virtual LAN (VLAN)

In questa lezione impareremo...

- le caratteristiche delle VLAN
- la differenza tra VLAN port based e tagged

Virtual LAN

Una Virtual LAN, meglio conosciuta come ◀ VLAN ▶, è una LAN realizzata *logicamente* grazie allo standard 802.1Q che definisce le specifiche che permettono di definire più reti locali virtuali (VLAN) distinte, utilizzando e condividendo una stessa infrastruttura fisica.

◀ Anche chiamata dominio di broadcast, è un segmento della rete all'interno del quale diversi host appartenenti a una stessa subnet comunicano tra di loro senza dover necessariamente passare da un router, appartenendo alla stessa VLAN. Prima della diffusione degli switch veniva utilizzato anche il termine dominio di collisione, tuttavia dato che lo switch elimina le collisioni, l'attenzione si è spostata sul traffico broadcast. ▶

Ciascuna VLAN si comporta come se fosse una rete locale separata dalle altre dove i pacchetti broadcast sono confinati all'interno di essa.

Possiamo affermare che la comunicazione a livello 2 è confinata all'interno della VLAN e la connettività tra diverse VLAN può essere realizzata solo a livello 3, attraverso il routing.

Le VLAN riguardano il livello 2 mentre le subnet interessano il livello 3: generalmente c'è una corrispondenza biunivoca tra VLAN e sottorete che viene definita con l'assegnazione delle porte dello switch, dato che la maggior parte degli switch moderni con un adeguato numero di porte sono in grado di gestire le VLAN.

In generale le VLAN consentono una maggiore agilità di manutenzione e modifica delle infrastrutture di rete, consentono di aggiungere dispositivi senza dover spostare cavi, riposizionare apparati di rete, semplicemente tramite strumenti software, inoltre riducono il traffico, isolando il broadcast. Vediamo i principali vantaggi delle VLAN.

- Economicità: attraverso uno switch di livello 3, è possibile effettuare routing tra le diverse VLAN.
- Scalabilità: l'espansione della rete diventa semplice ed economica, le VLAN si possono estendere su diversi switch, spostando semplicemente una porta o un cavo patch.
- Ottimizzazione dell'uso delle infrastrutture: per isolare una subnet non è necessario aggiungere uno switch e/o un router, ma riassegnare alcune porte.
- Possibilità di estensione oltre i limiti fisici di un singolo switch: una LAN può venire estesa, ad esempio su piani diversi, utilizzando un'unica dorsale di collegamento.

Usare una VLAN per isolare ad esempio il DMZ dalla Trusted LAN, potrebbe essere vulnerabile a un attacco di tipo Spoofing. Esistono diversi tipi di attacco a questo livello, sostanzialmente però tutti tendono a catturare i dati che passano su VLAN diverse, sfruttando eventuali configurazioni errate presenti sulle porte di trunk. Le porte di trunk, come vedremo, hanno accesso ai dati di tutte le VLAN. Per isolare le zone di una LAN è preferibile utilizzare, come vedremo in seguito, un firewall.

Realizziamo una VLAN

Per realizzare una VLAN è necessario che gli switch della infrastruttura di rete siano capaci di distinguere le diverse VLAN esistenti: questo avviene per mezzo dello standard 802.1Q.

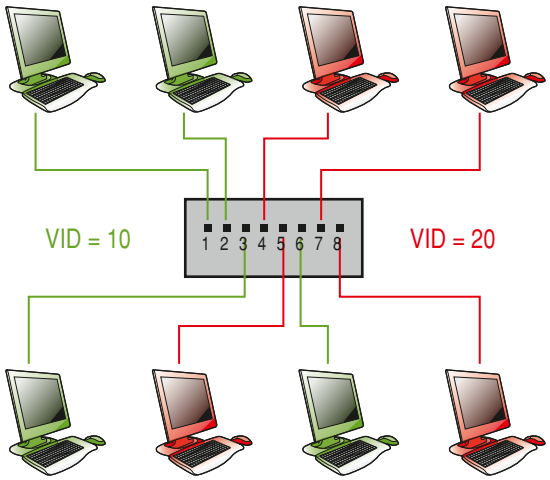
La realizzazione di VLAN può avvenire secondo due modalità:

- VLAN port based (untagged LAN o private VLAN);
- VLAN tagged (802.1Q).

Le VLAN vengono distinte, le une dalle altre, attraverso un nome, un numero identificativo chiamato VID (Virtual Identificator), compreso tra 1-4094 e un proprio blocco di indirizzi IP.

Una delle applicazioni più semplici realizzate tramite una VLAN è quella di "tagliare" un unico switch fisico in due o più reti diverse.
La figura seguente mostra due reti isolate attraverso l'utilizzo di un unico switch:

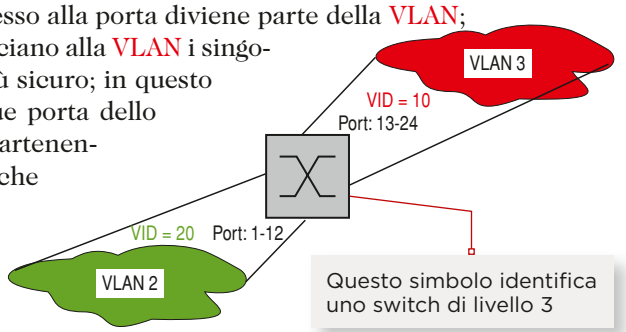
A la rete rossa è una VLAN con VID 20 e collega i 4 host (porta 4,5,7,8);
B la rete verde è una VLAN con VID 10 e collega i 4 host (porta 1,2,3,6).



Gli host di colore verde "vedono" soltanto gli host di colore verde, così come gli host rossi "vedono" solo quelli rossi. Senza la presenza di una VLAN sarebbe necessario utilizzare due switch diversi, uno per ogni VLAN.

Una volta definita una VLAN, ci sono sostanzialmente due tecniche per associarvi degli host:

- usando i numeri di porta dello switch: potremmo decidere che la prima metà delle porte è riservata agli host della VLAN 20 e le rimanenti per quelli della VLAN 10; questo è il sistema più semplice ma ha grossi limiti di sicurezza in quanto il concentratore associa una sua porta alla VLAN e non a un host: qualunque "dispositivo" venga connesso alla porta diviene parte della VLAN;
- usando gli indirizzi di rete degli host: se si associano alla VLAN i singoli indirizzi degli host si realizza un sistema più sicuro; in questo caso un host viene collegato a una qualunque porta dello switch dato che viene riconosciuta la sua appartenenza alla VLAN o per mezzo del suo indirizzo IP, che sappiamo però poter essere modificabile in qualsiasi momento, oppure l'indirizzo MAC, che è unico e immutabile per ogni interfaccia.



ESEMPIO

Switch a 48 porte

Se abbiamo a disposizione uno switch a 48 porte potremmo assegnare le porte nel modo seguente:

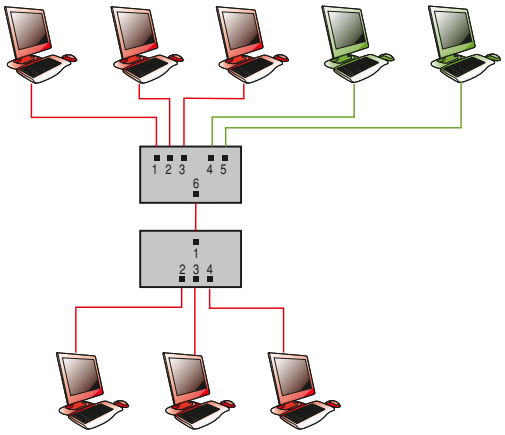
- le porte da 1 a 30 per la VLAN principale, con i client e i server di dominio (ad esempio rete alunni);
- le porte da 31 a 35 per una VLAN di stampanti con routing verso la LAN;
- sulle porte restanti si potrebbe definire una VLAN completamente separata per ospitare una rete riservata ai docenti e/o alla segreteria, che non si vuole condividere con il resto della popolazione scolastica.

Port based VLAN (untagged)

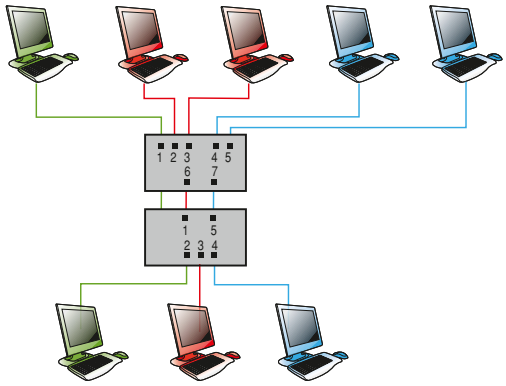
Questo metodo utilizza i numeri delle porte dello switch per realizzare VLAN differenti. Ciascuna porta prende anche il nome di Access port.

ESEMPIO

In questo esempio abbiamo due VLAN, una delle quali è limitata a un singolo switch.



In questo secondo esempio abbiamo tre VLAN e ciascuna crea una connessione "virtuale" tra i due switch.



Le operazioni che devono svolgere gli switch sono particolarmente semplici:

- ingress: un frame in ingresso appartiene alla VLAN a cui è assegnata la porta, quindi non è richiesto nessun altro "meccanismo "di riconoscimento di appartenenza sul frame;
- forwarding: il frame può essere inoltrato solo verso porte appartenenti alla stessa VLAN a cui appartiene la porta di ingresso che è mappato in un forwarding database, distinto per ogni VLAN;
- egress: una volta determinata la porta (o le porte) attraverso cui deve essere trasmesso il frame, questo può essere trasmesso così come è stato ricevuto, senza che venga modificato.

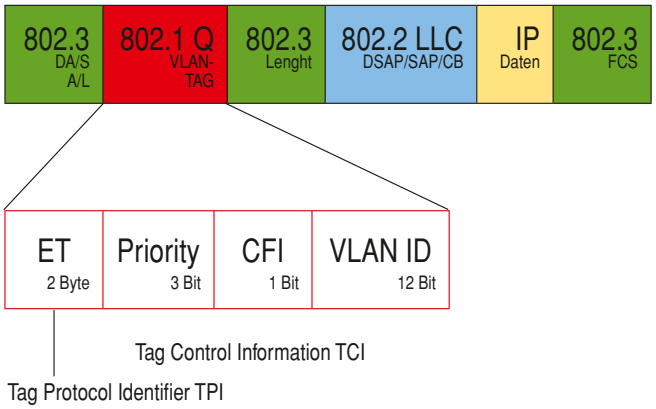
VLAN 802.1Q (tagged VLAN)

La tecnologia che permette di far condividere una VLAN a due o più switch mediante una modifica del formato del frame ethernet è quella che utilizza lo standard 802.1Q, la quale aggiunge 4 byte (TAG) che trasportano le informazioni sulla VLAN e altre aggiuntive. Ciascuna porta tagged prende anche il nome di porta di Trunk.

> Quando un pacchetto con tag VLAN n entra in una porta tagged se quella porta è tagged VLAN n, viene fatto passare, altrimenti viene scartato. Una volta che il pacchetto entra su una porta tagged può essere indirizzato solo sulle porte tagged e untagged della stessa VLAN n; se il pacchetto esce da una porta tagged sarà taggato come VLAN n, se invece esce da una porta untagged sarà privato del VLAN tag.

I primi 2 byte sono chiamati Tag Protocol Identifier (TPI) e contengono il tag EtherType (valore 0x8100), numero che evidenzia il nuovo formato del frame. I successivi 2 byte sono chiamati Tag Control Information TCI (o VLAN Tag), così strutturati:

- user_priority: campo a 3 bit che può essere utilizzato per indicare un livello di priorità per il frame;
- CFI: campo di 1 bit che indica se i MAC address nel frame sono in forma canonica;
- VID: campo di 12 bit che indica l'ID delle VLAN; con 12 bit possono essere definite 4096 VLAN: la prima (VLAN 0) e l'ultima (VLAN 4095) sono riservate, quindi gli ID realmente usabili sono 4094.

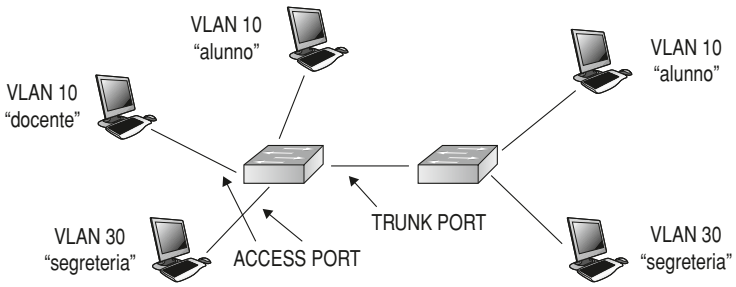


> Con queste "aggiunte" è possibile che il frame possa superare la lunghezza di 1518 byte, limite massimo dello standard Ethernet: gli switch che ammettono standard 802.1Q devono poter accettare frame con 2 byte in più.

I pacchetti con questo formato non possono arrivare su qualsiasi porta dello switch in quanto questo deve essere in grado di interpretarli: è necessario avere una classificazione anche delle porte, che possono essere distinte in porte trunk/tagged e porte untagged:

- se la porta è associata a una VLAN "port based" (untagged) i frame ricevuti da quella porta non necessitano (e non trasportano) tag TPI e TCI, né dovranno trasportarla i frame in uscita; queste porte sono chiamate porte d'accesso (access port) e il link attestato su tali porte si dice access link;
- se la porta è associata a una o più VLAN in modalità tagged, i frame trasporteranno le informazioni di TAG e la VLAN di appartenenza del frame è definita dal valore inserito nel TAG: queste porte sono chiamate porte Trunk e il link associato a tali porte si dice trunk link.

Osservando la rete rappresentata nella figura possiamo sicuramente affermare che le porte che connettono i due switch devono essere trunk in quanto in esse circoleranno frame di più VLAN.



Porte ibride

Lo standard VLAN 802.1Q richiede che una porta deve poter essere utilizzata in entrambe le modalità cioè deve poter essere associata a una VLAN in modalità untagged oppure ad altre VLAN in modalità tagged: in questo caso si parla di hybrid port.
Questa porta, come primo passo, riconosce se nel frame vi sono i tag TGI e TCI: se questi non sono presenti, il frame è del tipo untagged e quindi la porta funzionerà in tale modalità, se invece sono presenti, questi vengono analizzati e la VLAN di appartenenza viene individuata dal valore del VID.

> La VLAN a cui la porta è associata in modalità untagged viene anche detta PVID (Private Vlan ID).

Le operazioni che devono svolgere gli switch in questi casi sono diverse da quelle descritte per le VLAN untagged:

- ingress: per prima cosa lo switch deve riconoscere il tipo di frame e identificare la VLAN di appartenenza e quindi:
  - se il frame è untagged, la VLAN di appartenenza è identificata con la VLAN a cui la porta è associata in modalità untagged;
  - se il frame è tagged, la VLAN di appartenenza viene identificata dai TAG;
- forwarding: una volta identificata la VLAN di appartenenza vengono applicate le regole di forwarding e viene identificata la porta di uscita:
- egress: in questo caso può essere necessario effettuare l'inserimento e la rimozione dei TAG:
  - se il frame in ingresso è di tipo 802.1Q e la porta in uscita è associata alla VLAN di appartenenza in modalità tagged, il frame viene inoltrato senza modifiche;
  - se il frame in ingresso è untagged e la porta in uscita è associata alla VLAN di appartenenza in modalità untagged, il frame viene inoltrato senza modifiche;
  - se il frame in ingresso è di tipo 802.1Q e la porta di uscita è in modalità untagged è necessario rimuovere la TPI e TCI prima di effettuare l'inoltro;
  - se il frame in ingresso è di tipo 802.3 e la porta di uscita è associata alla VLAN di appartenenza in modalità tagged è necessario inserire TPI e TCI prima di effettuare l'inoltro.

> Negli ultimi due casi lo switch deve ricalcolare il valore del CRC del frame prima di ritrasmetterlo.

Naturalmente in una rete possono coesistere apparati che non supportano il protocollo 802.1Q: questi saranno connessi su porte dello switch associate esclusivamente a una VLAN in modalità untagged in modo che ogni frame ricevuto sarà associato a una VLAN e nessun frame di tipo 802.1Q sarà inoltrato verso l'apparato a valle, in quanto prima di arrivare al frame vengono rimossi i TAG.
In questo modo non è necessario sostituire tutto l'hardware esistente nel caso si voglia realizzare una VLAN: basta inserire in modo opportuno solo alcuni apparati 802.1Q e integrarli con l'hardware esistente, senza doverlo sostituire.
Anche le schede di rete presenti sugli host devono essere compatibili, e generalmente non lo sono: deve inoltre essere installato l'apposito driver e, infine, è necessario che il sistema operativo fornisca la possibilità di utilizzare le VLAN.

> È buona norma non utilizzare le VLAN per isolare le diverse zone della rete, ad esempio per ospitare una DMZ, perché il traffico tra le VLAN è spoofabile, cioè facilmente falsificabile: è quindi sempre meglio affidarsi a un firewall per isolare le zone tra le quali la sicurezza del traffico è un fattore critico.

Verifichiamo le conoscenze

1. Risposta multipla

1 Quale standard definisce le virtual LAN?

a. Standard 802.1L
b. Standard 802.1P
c. Standard 802.1Q
d. Standard 802.1V

2 Le VLAN sono in grado di:

a. consentire a postazioni attestate su segmenti di rete fisicamente distinti, di apparire connessi alla stessa rete logica
b. consentire a postazioni attestate su segmenti di rete fisicamente distinti, di apparire connessi alla stessa rete fisica
c. separare postazioni che sono sulla stessa rete fisica in più reti logiche distinte
d. separare postazioni che sono sulla stessa rete logica in più reti fisiche distinte

3 I principali vantaggi che derivano dall'utilizzo delle VLAN sono (indicare quelli errati):

a. risparmio
b. aumento di prestazioni
c. riduzione di occupazione di memoria
d. aumento della sicurezza
e. aumento della velocità di trasmissione
f. flessibilità

4 Il VID ha range:

a. 0-105
b. 1-105
c. 5-105
d. 0-1005
e. 1-1005
f. 5-1005

5 Per poter gestire più VLAN sulla stessa struttura fisica gli switch devono svolgere le funzioni di:

a. ingress
b. forwarding
c. wireless
d. espress
e. egress

6 I primi byte aggiunti nelle tagged VLAN sono chiamati:

a. Tag Protocol Identifier (TPI)
b. Tag Control Information TCI (o VLAN Tag)
c. Tag VLAN Definition (o VLAN Tag)
d. Tag Data Information TDI

2. Vero o falso

1 La VLAN permette a computer anche collocati in luoghi non vicini fisicamente di comunicare come se fossero sullo stesso *dominio di collisione*. V F
2 La connettività tra diverse VLAN può essere realizzata a livello 2. V F
3 Una utenza può vedere solo il traffico della propria VLAN e non delle altre. V F
4 Il VID distingue le VLAN port based da quelle VLAN tagged. V F
5 Nelle VLAN è preferibile utilizzare l'indirizzo IP piuttosto che il MAC per riconoscere un host. V F
6 Le VLAN che utilizzano i numeri di "porta" dello switch prendono il nome di Port based LAN. V F
7 Nelle VLAN untagged tutta la gestione è fatta all'interno dello switch. V F
8 Nelle VLAN trunking vengono aggiunti 4 byte al frame ethernet. V F
9 Il frame VLAN non deve comunque superare la lunghezza massima del frame ethernet. V F
10 La VLAN a cui la porta è associata in modalità untagged viene anche detta PVID. V F
11 Sono presenti quattro casi nei quali lo switch deve ricalcolare il valore del CRC del frame. V F

LEZIONE 2

Il protocollo VTP e l'Inter-VLAN Routing

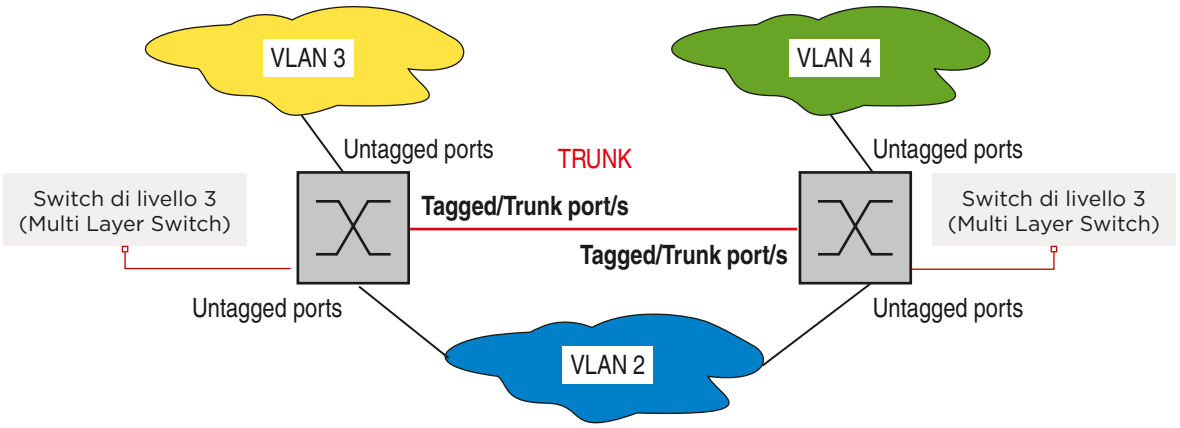
In questa lezione impareremo...

- il protocollo VTP
- la configurazione delle VLAN
- l'Inter-VLAN Routing

VLAN condivise su più di uno switch

La suddivisione di una rete in VLAN risponde da una parte a motivi di sicurezza, poiché diminuisce le possibilità di accesso indebito, dall'altra a motivi di prestazioni della rete, in quanto riduce il numero degli hops per il router, aumenta l'ampiezza di banda per il singolo utente e riduce il traffico broadcast.

Una VLAN può essere estesa a due o più switch proprio come una normale LAN e ogni switch presente nella rete LAN deve essere configurato; se la LAN ha dimensioni elevate è evidente come la gestione risulti complessa e inoltre possano facilmente essere introdotti degli errori.



◀ Con il termine trunk si intende la connessione punto-punto tra due porte trunk di uno switch. ▶

I frame che attraversano un ◀ trunk ▶ sono tutti "tagged" a eccezione di quelli appartenenti alla Native VLAN, che viene usata solo per il traffico di controllo.

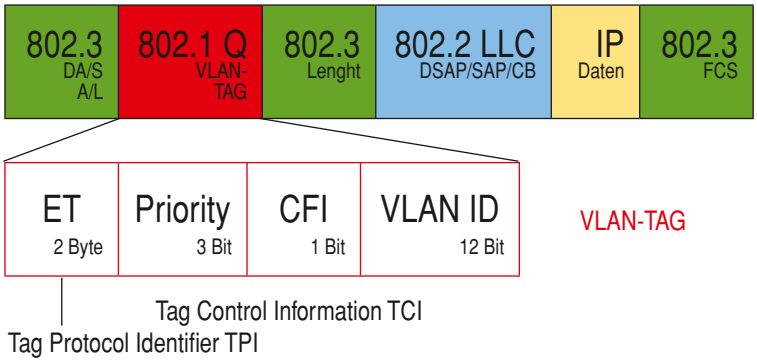
La configurazione della Native VLAN è la seguente:

```
Switch (config)# interface FastEthernet o/x
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk native vlan 99
```

Di default la porta trunk accetta tutte le VLAN ma è anche possibile configurare solo un sottoinsieme di VLAN consentite su un trunk con il comando:

```
Switch (config-if)# switchport trunk allowed vlan y
```

La tecnologia che permette di far condividere una VLAN a due o più switch è detta VLAN trunking e sappiamo che si avvale di un preambolo di 4 byte, il VLAN-TAG, aggiunto al pacchetto prima della "parte" 802.3.



Quindi due switch si connettono tra loro con una porta trunk di tipo tagged in modo da condividere e gestire più VLAN in comune: ogni switch deve essere opportunamente configurato.

Cisco VTP-VLAN Trunking Protocol

Il protocollo Virtual Trunking Protocol (VTP), proprietario della CISCO, consente di configurare le VLAN su un solo switch, che si occupa poi di distribuire le VLAN a tutti gli switch della rete: quindi riduce drasticamente la configurazione manuale degli switch.

VTP può essere configurato su Switch Cisco in tre modalità:
- Client;
- Server;
- Transparent.

Solo sugli switch in modalità "Server" l'amministratore di rete può modificare la configurazione delle VLAN. Quando viene fatta una modifica questa automaticamente viene distribuita a tutti gli switch del trunk VLAN:
- gli apparati in modalità "Transparent" reinviano le modifiche a tutti gli altri apparati a esso collegati;
- gli apparati in modalità "Client" prima applicano la modifica a se stessi e quindi la reinviano.

L'informazione viene propagata in base a mappe di raggiungibilità che l'algoritmo Spanning Tree (ST) ha costruito in maniera automatica.
Ogni modifica viene numerata con un config revision e ogni apparato in modalità Client applica la modifica a se stesso solo se risulta avere un version number maggiore di quello attuale: se si aggiunge un nuovo componente alla VLAN si deve ripartire da zero per evitare conflitti e quindi tutti i version number vengono resettati.

Il comando che consente di valutare la configurazione VTP di uno switch è

```
Switch# show vtp status
```

```
Switch0>show vtp status
VTP Version                     : 2
Configuration Revision          : 4
Maximum VLANs supported locally : 255
Number of existing VLANs        : 7
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xFC 0xCA 0xC6 0x4B 0x09 0x14 0x7E 0x79
Configuration last modified by 0.0.0.0 at 3-1-93 00:22:37
Local updater ID is 0.0.0.0 (no valid interface found)
Switch0>
```

I parametri da configurare sono:

VTP version: esistono tre versioni del protocollo VTP (1, 2 e 3); di default la versione 1 e, solo nei dispositivi più recenti, la 2;

VTP mode: sono le tre modalità prima descritte (Client, Server, Transparent); di default uno switch si trova in modalità Server;

VTP Domain Name: un VTP Domain è un insieme di switch che si scambiano VTP advertisement per la distribuzione delle VLAN e uno switch può appartenere a un solo dominio VTP alla volta; il valore di default per il VTP Domain Name è "null";

Zoom su...

VTP ADVERTISEMENT

Un messaggio VTP è inviato ogni volta che bisogna propagare informazioni sulle VLAN: esistono tre tipi di VTP Advertisement:

- summary: contengono il VTP Domain Name e il Config Revision: sono inviate ogni 5 minuti e hanno lo scopo di informare i vicini del corrente VTP Config Revision;
- subset: contengono informazioni sulle VLAN (inserimento, cancellazione, modifica);
- request: inviate a un VTP server per richiedere l'invio di un messaggio Summary e di eventuali messaggi subset.

Config Revision: è un contatore inizialmente impostato a zero che viene incrementato di uno ogni qual volta si verifica una modifica, cioè se viene aggiunta o rimossa una VLAN, in modo che gli switch sono in grado di valutare se le informazioni VTP memorizzate sono o meno aggiornate.

I comandi per modificarne i valori iniziano con vtp seguito semplicemente dal nome dell'opzione e dal valore alla quale deve essere settato:

```
Switch0(config)#vtp ?
  domain     Set the name of the VTP administrative domain.
  mode       Configure VTP device mode
  password   Set the password for the VTP administrative domain
  version    Set the adminstrative domain to VTP version
Switch0(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch0(config)#
```

Configurazione delle VLAN

Per creare una VLAN si procede con le seguenti operazioni:
a) ci si collega via Telnet allo switch;
b) si accede mediante il comando `Configure terminal`;
c) il prompt diventerà `nomeswitch (config)#`;
d) con il comando VLAN `{id_vlan}` si assegna un numero identificativo alla nuova VLAN diverso da 1, dato che la VLAN 1 è quella cui per default sono assegnate tutte le porte dello switch.

ESEMPIO

Definiamo la VLAN con VID 10 e configuriamo un host con nome docente, come in figura:

```
Switch (config)# VLAN 10
```

È utile ai fini pratici assegnare anche un nome con il comando:

```
Switch (config)# name docente
```

Terminata la creazione, si esce dal Global configuration mode con exit.

Per verificare le operazioni effettuate si utilizza il comando:

```
Switch (config)# show vlan
```

Per salvare la configurazione si utilizza il comando:

```
Switch# copy running-config startup-config
```

Riepiloghiamo la sequenza di operazioni che ci permette di creare la VLAN 20, assegnarle il nome alunni e aggiungerla al database delle VLAN.

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# name alunni
Switch(config-vlan)# end
Switch# show vlan
Switch# copy running-config startup-config
```

È possibile portare rettifiche ai parametri di una VLAN sempre utilizzando i sopra elencati comandi; è inoltre possibile eliminare una VLAN tramite il comando:

```
Switch(config)# no vlan 20
```

sempre digitandolo nel Global configuration mode.

Naturalmente, a cancellazione avvenuta, la configurazione deve essere salvata con il solito copy running-config startup-config. In modo analogo si procede nel VLAN configuration mode.

Per assegnare una porta a una VLAN si definisce prima l'interfaccia che si vuole assegnare alla VLAN, si precisa la modalità per la porta e quindi si assegna la porta.

I seguenti comandi ci permettono di assegnare alla VLAN 20 la porta 0/1:

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1     // scelta dell'interfaccia
Switch(config-if)# switchport mode access // modalità per la porta
Switch(config-if)# switchport access vlan 20  // assegnazione della porta
Switch(config-if)# end
```

Per verificare la corretta configurazione della porta si utilizza il comando:

```
Switch# show running-config interface fastethernet0/1
```

mentre per verificare l'assegnazione della porta si utilizza:

```
Switch# show interface fastethernet0/1
```

Per salvare la configurazione si utilizza il comando:

```
Switch# copy running-config startup-config
```

Inter-VLAN Routing

Le VLAN possono estendersi al di là dei limiti fisici dei singoli switch, tramite il VLAN tagging: la VLAN coinvolge quindi dei router, che devono essere appositamente configurati.

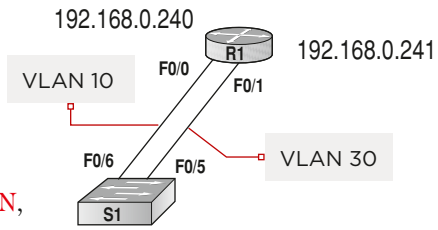
> Anche per consentire la comunicazione tra VLAN diverse è necessario introdurre nella LAN un router o uno switch di livello 3.
> In questo caso si parla di inter-VLAN Routing.

Il protocollo 802.1Q, che regola le VLAN, prevede che ciascun frame ethernet venga "etichettato" con le informazioni relative alla VLAN di appartenenza.

Sono disponibili tre soluzioni:
- Inter-VLAN tradizionale;
- "Router-on-a-stick" Inter-VLAN;
- Switch-based Inter-VLAN.

Inter-VLAN tradizionale

Per far cominciare due VLAN il modo più semplice è quello di inserire un router e connetterlo a uno degli switch della LAN: la connessione tra il router e lo switch deve essere fatta con un numero di interfacce fisiche pari al numero delle VLAN che devono poter comunicare tra di loro. ▶



Dato che a ogni interfaccia fisica del router è associata a una VLAN, questa deve avere un indirizzo IP appartenente a tale VLAN.

> Le porte dello switch connesse al router devono essere impostate in modalità access.

Vediamo come deve essere la corretta configurazione delle interfacce del Router con la corretta assegnazione degli indirizzo IP:

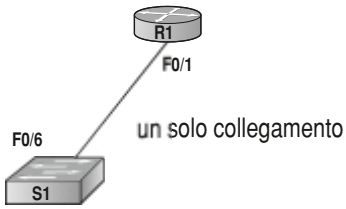
```
R1(config)# interface Fa 0/0
R1(config-if)#ip address 192.168.0.240 255.255.255.0
R1(config-if)# no shutdown
R1(config)# interface Fa 0/1
R1(config-if)#ip address 192.168.0.241 255.255.255.0
R1(config-if)# no shutdown
```

Sullo switch configuriamo le interfacce delle porte connesse al router in modalità access seguita dalla indicazione del nome della VLAN:

```
S1(config)# vlan 10
S1(config)# interface Fa 0/6
S1(config-if)# switchport access vlan 10
S1(config)# vlan 30
S1(config)# interface Fa 0/5
S1(config-if)# switchport access vlan 30
```

"Router-on-a-stick" Inter-VLAN

In questo caso il router viene connesso a uno degli switch della LAN con una sola interfaccia fisica. ▶



Opereremo una "suddivisione" dell'interfaccia fisica in tante interfacce virtuali quante sono le VLAN che possono comunicare tra di loro: ogni interfaccia virtuale (subinterface) del router è associata a una VLAN e deve quindi avere un indirizzo IP appartenente a tale VLAN.

La porta dello switch connessa al router deve essere impostata in modalità trunk.

ESEMPIO

Supponiamo di avere tre VLAN, (vlan10, vlan20 e vlan30): l'interfaccia del router che lo connette allo switch deve essere suddivisa in 3 subinterfaces e a ogni subinterface deve essere associata una VLAN.

```
R1(config)# interface Fa 0/0.10
R1(config-if)# encapsulation dot1q 10
R1(config-if)#ip address 192.168.0.240 255.255.255.0
R1(config)# interface Fa 0/0.20
R1(config-if)# encapsulation dot1q 20
R1(config-if)# ip address 192.168.0.240 255.255.255.0
R1(config)# interface Fa 0/0.30
R1(config-if)# encapsulation dot1q 30
R1(config-if)# ip address 192.168.0.240 255.255.255.0
R1(config)# interface Fa 0/0
R1(config-if)# no shutdown
```

Sullo switch configuriamo le interfacce delle porte connesse al router in modalità trunk:

```
S1(config)# vlan 10
S1(config)# vlan 20
S1(config)# vlan 30
S1(config)# interface Fa 0/1
S1(config-if)# switchport mode trunk
```

Verifichiamo le conoscenze

1. Risposta multipla

1 La suddivisione di una rete in VLAN (indica la motivazione errata):

a. diminuisce le possibilità di accesso indebito
b. riduce il numero degli hops per il router
c. aumenta l'ampiezza di banda per il singolo utente
d. riduce le possibilità di errore di indirizzamento
e. riduce il traffico broadcast

2 VTP può essere configurato su Switch Cisco in tre modalità:

a. Client
b. Server
c. Hybrid
d. Transparent

3 I parametri VTP da configurare sono (indica quello errato):

a. VTP version
b. VTP configuration revision
c. VTP mode
d. VTP Domain

4 Esistono tre tipi di VTP Advertisement:

a. summary
b. subset
c. request
d. responce

5 Quale tra i seguenti parametri non è messaggio contenuto nel subset?

a. Inserimento
b. Cancellazione
c. Modifica
d. Configurazione

2. Ordinamento

1 Ordina la sequenza di operazioni necessarie per assegnare una porta a una VLAN:

a. ..... si assegna la porta.
b. ..... si definisce l'interfaccia
c. ..... si precisa la modalità per la porta

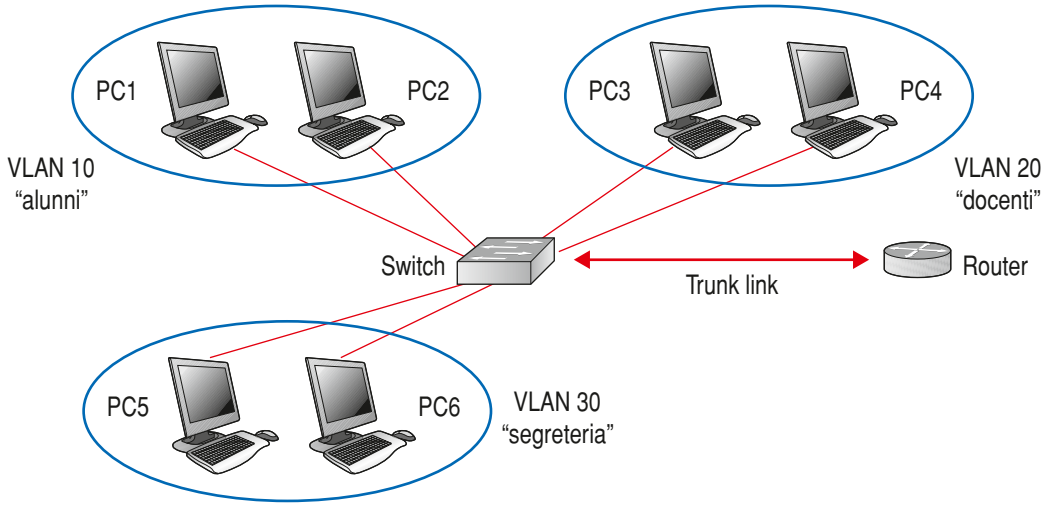
3. Vero o falso

1 Con il termine trunk si intende la connessione punto-punto tra due porte trunk di un router. V F
2 I frame che attraversano un trunk sono tutti "tagged". V F
3 Solo sugli switch in modalità "Server" si può modificare la configurazione delle VLAN. V F
4 Il "version number" indica la versione del VTP negli switch Cisco. V F
5 Esistono tre versioni del protocollo VTP; di default è configurato a 2. V F
6 Uno switch può appartenere a un solo dominio VTP alla volta. V F
7 Il comando "copy running-config startup-config" serve per fare una copia di backup. V F
8 Il VLAN tagging permette di estendersi al di là dei limiti fisici dei singoli switch. V F
9 Nell'Inter-VLAN tradizionale le porte dello switch sono connesse al router. V F
10 Nella "Router-on-a-stick" la porta dello switch connessa al router deve essere trunk. V F

Verifichiamo le competenze

1. Esercizi

1 Data la topografia di rete di figura si configuri lo switch seguendo le indicazioni dei commenti:



Soluzione

Prima di procedere alla configurazione dello switch assegniamo le porte alle funzioni preposte, come segue:

Porta 16	VLAN 1
Porta 17	
Porta 18	VLAN 2
Porta 19	
Porta 22	VLAN 3
Porta 23	
Porta 20	Porta TRUNK

```
configure terminal
.....................................
.....................................    crea ID VLAN1 e assegna il nome
end

.....................................
.....................................    crea ID VLAN2 e assegna il nome
end

.....................................
.....................................
.....................................    crea ID VLAN3 e assegna il nome
end
.....................................    salva la configurazione
.....................................    verifica la configurazione
.....................................
.....................................    0/16 configurazione VLAN1 sulla porta 16
```

```
.....
.....
end
.....    salva configurazione VLAN1 porta 16

.....
.....    0/17 configurazione VLAN1 sulla porta 17
.....
.....
end
.....    salva configurazione VLAN1 porta 17

.....
.....    configurazione VLAN2 sulla porta 18
.....
.....
end
.....    salva configurazione VLAN2 porta 18

.....
.....    configurazione VLAN2 sulla porta 19
.....
.....
end
.....    salva configurazione VLAN2 porta 19

.....
.....    configurazione VLAN3 sulla porta 22
.....
.....
end
.....    salva configurazione VLAN3 porta 22

.....
.....    configurazione VLAN3 sulla porta 23
.....
.....
end
.....    salva configurazione VLAN3 porta 23

.....
.....
.....    assegnazione della porta 20 all'accesso di tipo trunk
end
.....    salva configurazione
```

Esercitazioni di Laboratorio 1

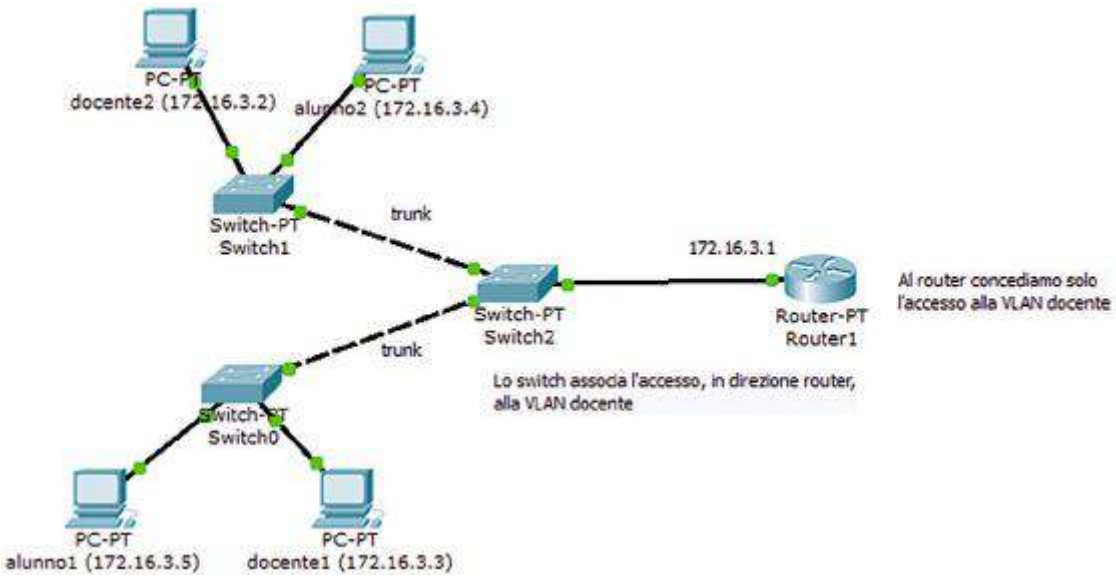
REALIZZIAMO UNA VLAN CON PACKET TRACER

VLAN

L'introduzione delle VLAN permette di far condividere lo stesso hardware a LAN diverse, isolandole tra loro, in modo tale da essere praticamente indipendenti. Le tecniche utilizzate per assegnare gli host alla rispettiva VLAN sono sostanzialmente tre:

- elenco dei MAC address;
- elenco degli indirizzi IP;
- settaggio della porta dello switch.

In questa lezione vogliamo utilizzare le VLAN per concedere l'accesso al router solo ad alcuni host. La rete presentata di seguito è formata da tre switch, un router e quattro host:

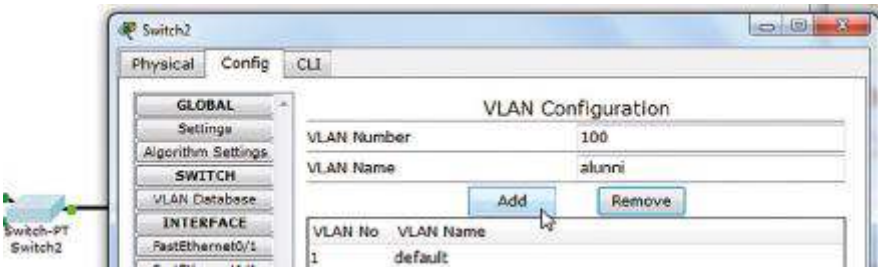


Vediamo la configurazione degli indirizzi degli host:
docente1 (172.16.3.3/16)
docente2 (172.16.3.2/16)
alunno1 (172.16.3.5/16)
alunno2 (172.16.3.4/16)

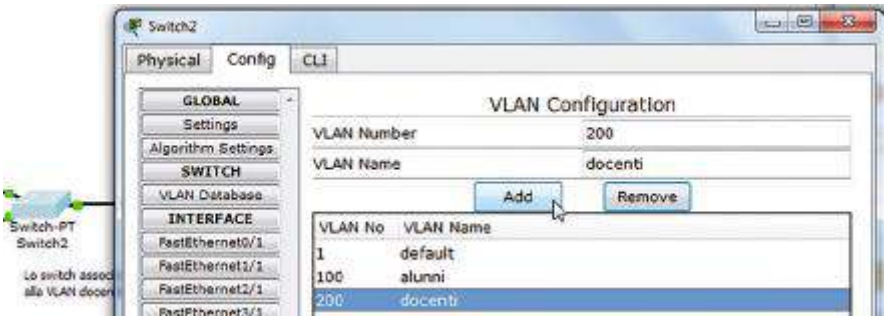
Per tutti gli host il gateway è rappresentato dall'indirizzo dell'interfaccia del router (Router1): 172.16.3.1

1. Vogliamo creare due VLAN: una VLAN alunni (numero: 100) e una VLAN docenti (numero: 200).

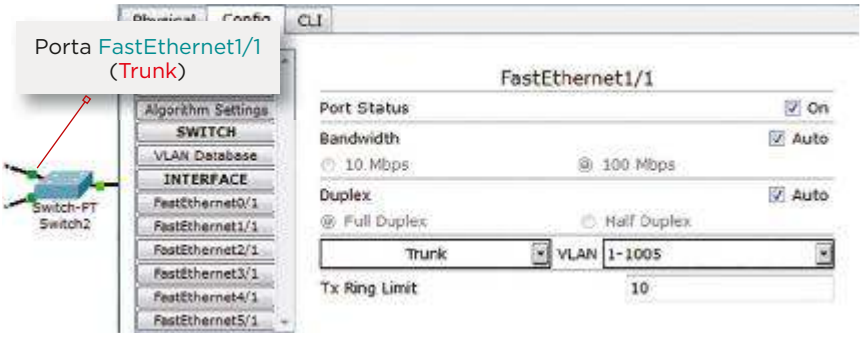
2 Per prima cosa andiamo a definire le VLAN dello Switch2: per fare questo facciamo clic sullo Switch2, scheda Config, poi facciamo clic su VLAN Database. Scriviamo 100 nella casella VLAN Number e alunni nella casella VLAN Name, quindi facciamo clic su Add:



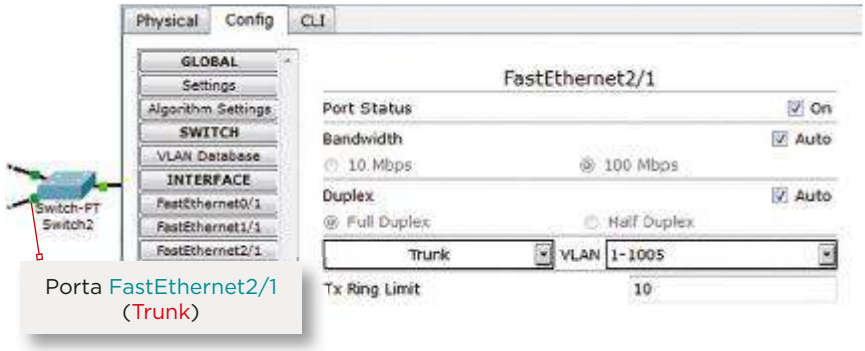
3 Quindi scriviamo 200 nella casella VLAN Number e docenti nella casella VLAN Name, facendo clic su Add andiamo ad aggiungere la seconda VLAN:



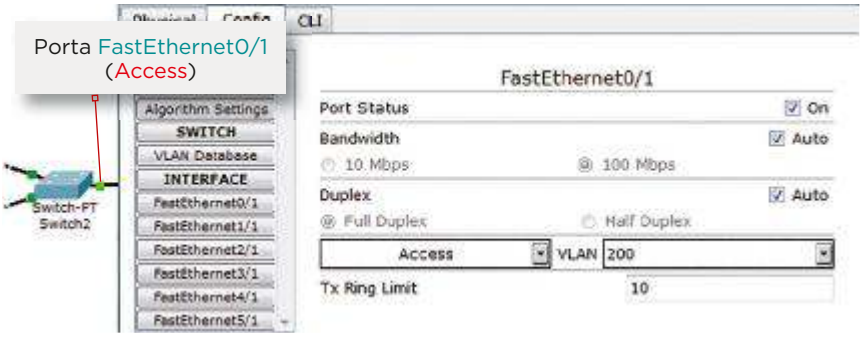
4 Passiamo a definire le singole porte dello switch2, iniziando dalla porta FastEthernet1/1, che deve essere di tipo Trunk:



5 Definiamo adesso la VLAN per la porta FastEthernet2/1, che deve essere configurata anch'essa in modalità Trunk:

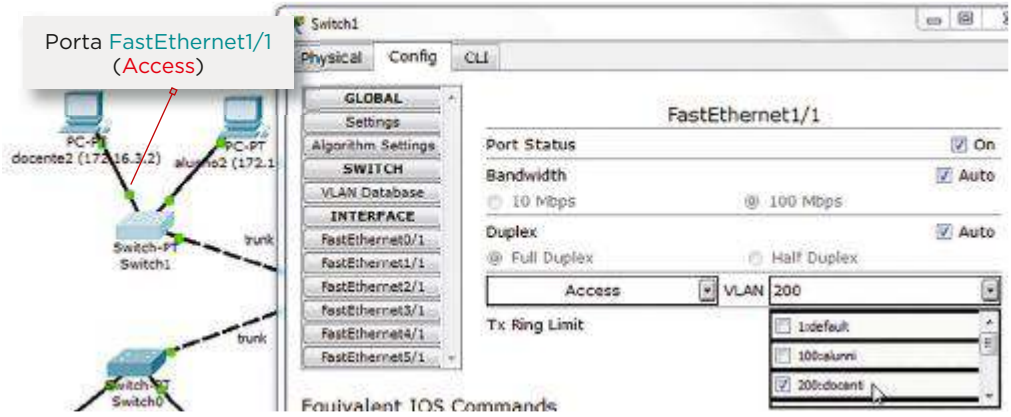


6 La porta FastEthernet0/1 collega lo Switch2 al router. Dobbiamo assegnare a questa porta la VLAN che fornisce l'accesso al router, cioè la VLAN dei docenti (200):

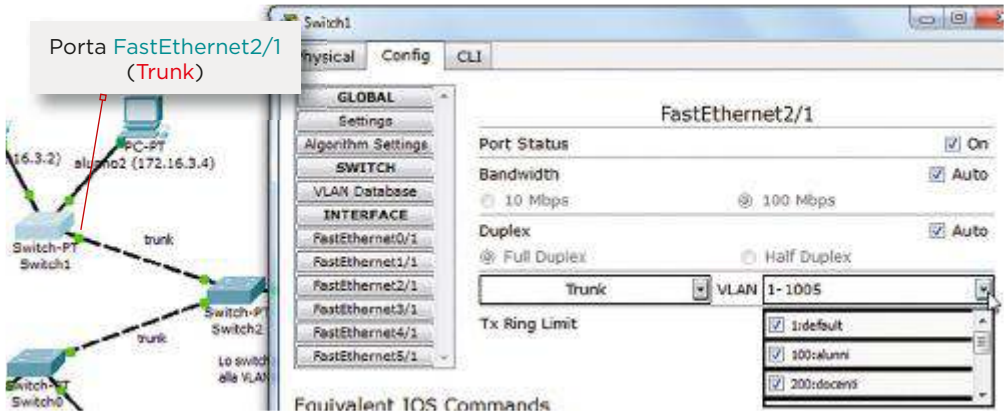


7 Passiamo a definire la porta FastEthernet0/1 dello Switch1. Assegniamo a questa porta la VLAN alunni (100):

8 Passiamo a definire la porta FastEthernet1/1 dello Switch1. Assegniamo a questa porta la VLAN docenti (200):

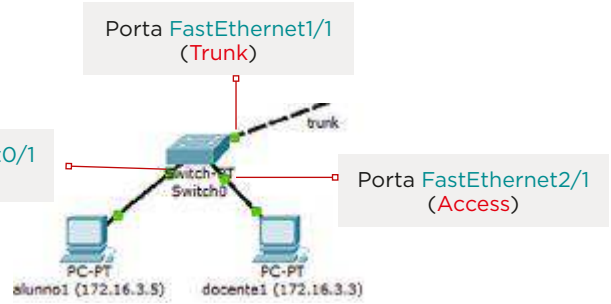


9 Passiamo a definire la porta FastEthernet2/1 dello Switch1. Assegniamo a questa porta la modalità VLAN di tipo Trunk, che possiamo notare abilita tutte le VLAN poste nell'elenco:



10 Configuriamo infine lo Switch0 nel modo seguente:

- porta FastEthernet1/1 Trunk
- porta FastEthernet0/1 VLAN alunni
- porta FastEthernet2/1 VLAN docenti



Prova adesso!

- Applicare le VLAN agli switch
- Settare le porte Trunk e Access

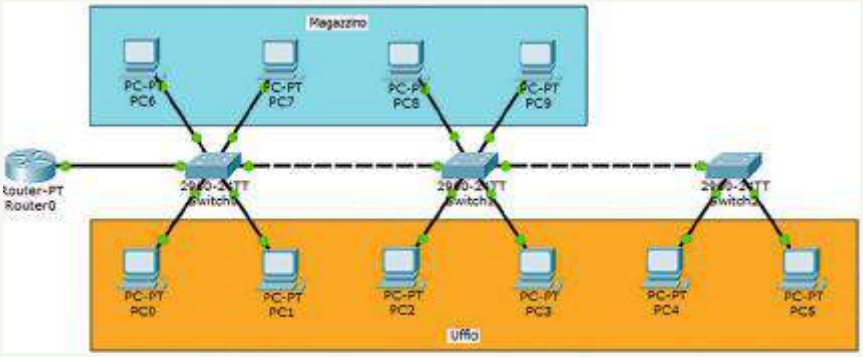
APRI IL FILE rete_VLAN.pkt

Modifica l'esempio verificando l'accessibilità al router da parte degli Host docente e la non accessibilità da parte degli Host alunno.

Prova adesso!

- Applicare le VLAN agli switch
- Settare le porte Trunk e Access

1 Crea una rete come indicato nella figura che segue:



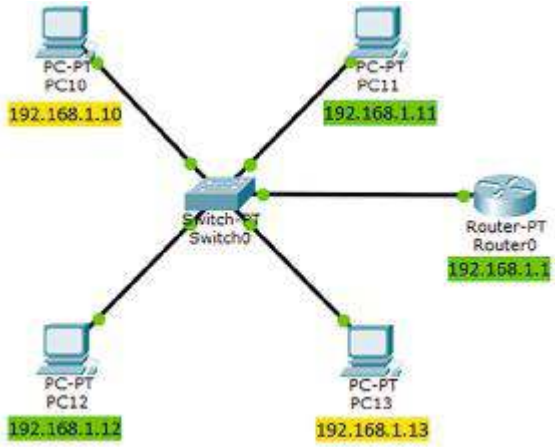
2 L'accesso al router deve essere consentito solo agli Host delle rete Uffici e non della rete Magazzino, utilizzando le VLAN.

Esercitazioni di Laboratorio 2

I COMANDI CLI PER CONFIGURARE LA VLAN

Definiamo due VLAN

Data la rete rappresentata nella figura seguente, vogliamo realizzare due VLAN, rispettivamente:
VLAN 10: connessione tra i PC 10 e PC 13 (VLAN alunni)
VLAN 20: connessione tra i PC 11 e PC 12 (VLAN docenti)



Clicchiamo sullo `switch` e selezioniamo la finestra config, quindi la scheda CLI e digitiamo i comandi seguenti.

Comandi VLAN untagged

COMANDO	DESCRIZIONE
`enable`	Entra in ambiente modalità privilegiata
`configure terminal`	Entra in modalità configurazione
`show vlan`	Elenca le VLAN presenti
`vlan 'id vlan'`	Crea una VLAN con un id scelto
`name 'nome'`	Assegna un nome a una nuova VLAN
`interface 'porta'`	Accede all'interfaccia della porta
`interface range 'porte'`	Accede a un range di porte
`switchport mode access`	Imposta la modalità della porta in untegged (access)
`switchport access vlan 'id vlan'`	Imposta la porta a cui fa riferimento la VLAN
`copy running-config startup-config`	Salva la configurazione dello switch

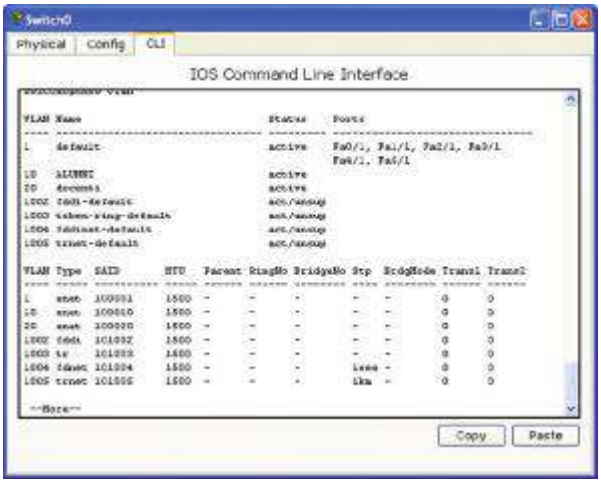
Comandi VLAN tagged

COMANDO	DESCRIZIONE
enable	Entra in ambiente modalità privilegiata
configure terminal	Entra in modalità configurazione
interface 'porta'	Accede all' interfaccia della porta (per le porte trunk usare 0/24)
switchport mode trunk	Imposta la modalità della porta in tagged (trunk)
switchport trunk allowed vlan add 'id vlan'	Imposta la porta in cui i dati possono transitare
copy running-config startup-config	Salva la configurazione dello switch

Vediamo i comandi IOS necessari per creare le VLAN indicate

```
Switch0>enable
Switch0#configure terminal
Switch0(config)# vlan 10
Switch0(config-if)# name ALUNNI
Switch0(config)# vlan 20
Switch0(config-if)# name docenti
Switch0(config-vlan)#exit
Switch0(config)#
```

Passiamo ora nella finestra CLI e digitiamo il comando show VLAN, otteniamo la finestra seguente:



Assegniamo ora le porte dello switch alle VLAN sapendo che:

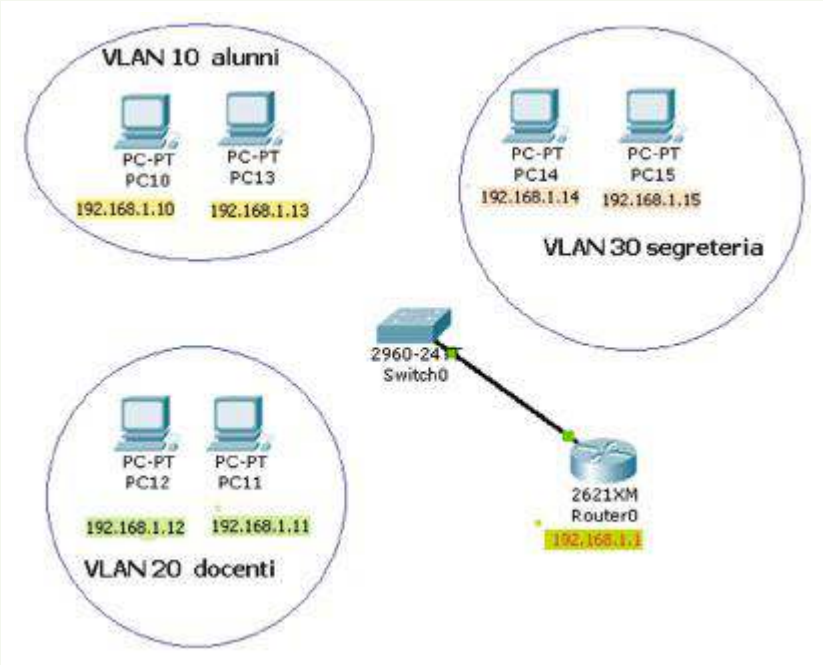
- il PC10 è connesso alla porta Fa0/1 e deve essere connesso alla VLAN10
- il PC13 è connesso alla porta Fa3/1 e deve essere connesso alla VLAN10
- il PC11 è connesso alla porta Fa2/1 e deve essere connesso alla VLAN20
- il PC12 è connesso alla porta Fa1/1 e deve essere connesso alla VLAN20

Scriviamo i comandi seguenti per assegnare alla porta 3/1 la VLAN alunni (10):

```
Switch0# configure terminal
Switch0(config)# interface fastethernet3/1
Switch0(config-if)# switchport access vlan 10
Switch0(config-if)# exit
```

Prova adesso!

Dopo aver realizzato la rete di figura, verificane il funzionamento provando la comunicazione tra i quattro PC prima e dopo la realizzazione delle VLAN.
Esegui un PING tra PC10 e PC11 e successivamente tra PC10 e PC12.
Allo stesso modo prova a pingare tra PC11 e PC12 e successivamente tra PC11 e PC13.
Cosa puoi osservare?
Quindi aggiungi una nuova VLAN, segreteria, con VID 30, come in figura.



Assegna le porte dello switch come indicato nella seguente tabella:

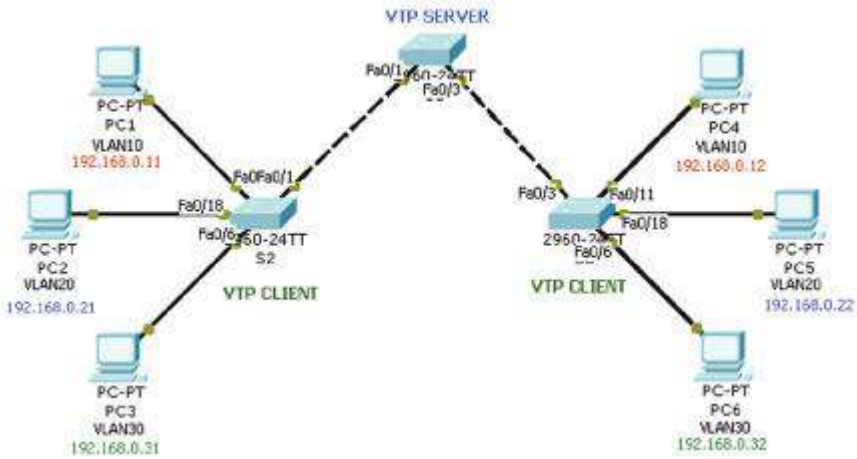
Porta 16	VLAN 1
Porta 17	
Porta 18	VLAN 2
Porta 19	
Porta 22	VLAN 3
Porta 23	
Porta 20	Porta TRUNK

Verifica il funzionamento sempre effettuando tutte le combinazioni di PING tar i diversi host.

Esercitazioni di Laboratorio 3

VLAN E VTP CON PACKET TRACER

Si vuole realizzare la rete di figura utilizzando il protocollo VTP.



Per prima cosa configuriamo il server.

Configurazione del VTP Server

Per prima cosa verifichiamo che lo switch abbia la configurazione di default con Config Revision uguale a 0:

```
Switch> show vtp status
```

```
Switch>show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 7
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xFC 0xCA 0xC6 0x4B 0x09 0x14 0x7E 0x79
Configuration last modified by 0.0.0.0 at 3-1-93 00:22:37
Local updater ID is 0.0.0.0 (no valid interface found)
Switch>
```

Di default lo switch ha l'Operation Mode in modalità server, quindi non deve essere modificato.

Passiamo in modalità config e assegniamo un nome dal dominio, ad esempio **scuola**:

```
Switch(config)# vtp domain scuola
```

Il nostro switch utilizza la versione 2 del protocollo: per modificarla si utilizza il comando:

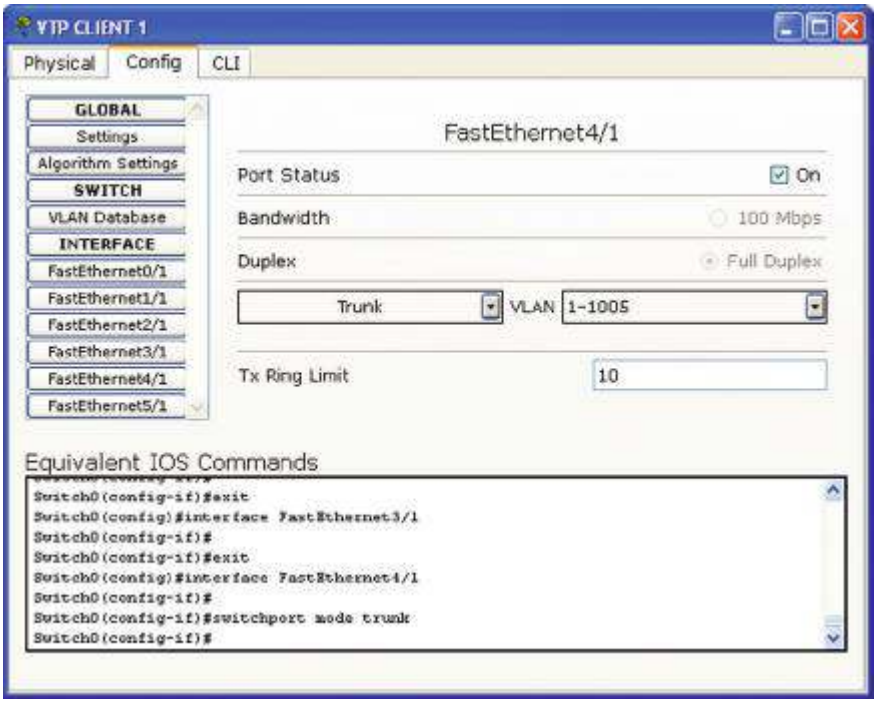
```
Switch(config)# vtp version 1
```

Configuriamo la password, ad esempio **itis**:

```
Switch(config)# vtp password itis
```

```
Switch#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vtp domain scuola
Changing VTP domain name from NULL to scuola
Switch(config)#vtp password itis
Setting device VLAN database password to itis
Switch(config)#
```

Come ultimo passaggio è necessario configurare le VLAN, popolando il VLAN database, e settare le porte trunk.



Configurazione del VTP Client

Anche sugli switch che fungeranno da client è necessario verificare che abbiano la configurazione di default con Config Revision uguale a 0:

```
Switch> show vtp status
```

Di default lo switch ha l'Operation Mode in modalità server, quindi deve essere modificato e settato come client:

```
Switch(config)# vtp mode client
```

```
Switch0(config)#vtp ?
  domain     Set the name of the VTP administrative domain.
  mode       Configure VTP device mode
  password   Set the password for the VTP administrative domain
  version    Set the adminstrative domain to VTP version
Switch0(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch0(config)#vtp mode client
Device mode already VTP CLIENT.
Switch0(config)#
```

Verifichiamo ora se l'interfaccia è in modalità trunk con il comando:

```
Switch# show interface FastEthernet4/1 switchport
```

otteniamo la seguente videata:

```
Switch0#show interface FastEthernet4/1 switchport
Name: Fa4/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
```

L'ultima operazione consiste nel configurare tutte le porte di accesso.

Prova adesso!

• Applicare le Virtual LAN

1 Completa la rete aggiungendo gli host in modo da definire quattro VLAN:
- VLAN 10 LABORATORIO1
- VLAN 20 LABORATORIO2
- VLAN 30 AULA
- VLAN 40 SEGRETERIA

collegando alcuni host di ciascuna rete a entrambi gli switch.
Al termine della configurazione verifica le funzionalità pingando tra i vari host.
Aggiungi in seguito una nuova VLAN, VLAN 50 MENSA, e verifica su tutti gli switch il valore di
Config Revision dopo aver collegato due host, uno per switch.

2 Modifica la rete dell'esercizio precedente sostituendo le seguenti quattro VLAN:
- VLAN 10 LAB_INFORMATICA1
- VLAN 20 LAB_INFORMATICA2
- VLAN 60 LAB_SISTEMI1
- VLAN 70 LAB_SISTEMI2

collegando alcuni host di ciascuna rete a entrambi gli switch.
Al termine della configurazione verifica le funzionalità pingando tra i vari host.
Riorganizza la rete in modo da separare fisicamente i laboratori dalla didattica.

CLIL

VLAN

A network of computers that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which makes them extremely flexible. One of the biggest advantages of VLANs is that when a computer is physically moved to another location, it can stay on the same VLAN without any hardware reconfiguration.

Virtual LAN

A virtual (VLAN) facilitates high-speed virtual Ethernet communications using memory and the system's processor rather than actual Ethernet cards. Used in Virtual I/O Servers, administrators can dynamically create virtual Ethernet segments or restrict access to VLAN segments. Virtual Ethernets are similar to physical Ethernets in that they support multiple networking protocols.

Virtual Ethernet can also refer to the virtual Ethernet (vEth) specification, a forthcoming standard that will provide access for network controls in virtualized environments comparable to the controls available in physical networks.

VLAN hopping

VLAN hopping is a computer security exploit, a method of attacking networked resources on a virtual LAN (VLAN). The basic concept behind all VLAN hopping attacks is for an attacking host on a VLAN to gain access to traffic on other VLANs that would normally not be accessible. There are two primary methods of VLAN hopping: switch spoofing and double tagging. Both attack vectors can be easily mitigated with proper switch port configuration.

Switch spoofing

In a switch spoofing attack, an attacking host imitates a trunking switch by speaking the tagging and trunking protocols (e.g. Multiple VLAN Registration Protocol, IEEE 802.1Q, Dynamic Trunking Protocol) used in maintaining a VLAN. Traffic for multiple VLANs is then accessible to the attacking host.

Double tagging

In a double tagging attack, an attacking host connected on a 802.1q interface prepends two VLAN tags to packets that it transmits. The packet (which corresponds to the VLAN that the attacker is really a member of) is forwarded without the first tag, because it is the native VLAN. The second (false) tag is then visible to the second switch that the packet encounters. This false VLAN tag indicates that the packet is destined for a target host on a second switch. The packet is then sent to the target host as though it originated on the target VLAN bypassing the network mechanisms that logically isolate VLANs from one another. However, this attack allows to send packets toward the second switch, but possible answers are not forwarded to the attacking host.

As an example of a double tagging attack, consider a secure web server on a VLAN called VLAN2. Hosts on VLAN2 are allowed access to the web server; hosts from outside VLAN2 are blocked by layer 3 filters. An attacking host on a separate VLAN, called VLAN1(Native), creates a specially formed packet to attack the web server. It places a header tagging the packet as belonging to VLAN2 under the header tagging the packet as belonging to VLAN1. When the packet is sent, the switch sees the default VLAN1 header and removes it and forwards the packet. The next switch sees the VLAN2 header and puts the packet in VLAN2. The packet thus arrives at the target server as though it was sent from another host on VLAN2, ignoring any layer 3 filtering that might be in place.

VLAN Insecurity

Virtual LANs (VLANs) make it possible to isolate traffic that shares the same switch, and even groups of switches. The switch designers had something other than security in mind when they added this form of isolation. VLANs make it possible to share a switch among many LANs, by filtering and limiting broadcast traffic. But this form of isolation relies on software and configuration, not the physical isolation that security people like to see.

In the last couple of years, some firewalls have become VLAN aware, so that policies can be created that rely on the tags that identify a packet as belonging to a particular VLAN. While firewalls that are VLAN aware add a lot of flexibility useful to Web hosting sites, the tags that these firewalls rely on were not designed with security in mind. VLAN tags can be created by devices other than switches, and valid tags that will fool the firewall can easily be added to packets.

Let's take a look at VLANs, including how they work, why this has little to do with security, and failures of VLANs to maintain isolation. And, if you decide to use VLANs as part of your security architecture, what you should do to minimize the weaknesses involved.

The term "switch" today denotes a device that switches network traffic between interfaces, named ports. But not too long ago, switches were

called bridges. Even today, if you read the IEEE standards used in switches, the term inevitably used is bridge. And if you are familiar with the way bridges work, you might want to skip ahead.

You use bridges to connect segments of the same LAN, that is, a local network that does not require routing. The bridge software learns which port that network devices have been connected to by examining the source MAC (Medium Access Control) addresses in the packets that the bridge passes. At first, the bridge knows nothing, and must distribute all the packets it receives to every port. But over time, the bridge learns how to send packets out the correct interface by building spanning trees, an algorithm developed for choosing the right interface and avoiding loops. By sending packets out on a single port, the bridge reduces overall network traffic. Think of the bridge in highway terms, something that connects different roads, and only passes necessary traffic between these roads.

Although the use of bridges does reduce overall network traffic, making networks more efficient, bridges still need to send broadcast packets to all ports. Just as in any LAN, broadcasts mean just that, a message broadcast to all systems. ARP (Address Resolution Protocol) packets provide an important example of broadcast messages.

As bridge hardware grew more capable, with increasing number of ports and the addition of management software, a new feature appeared. You could partition a bridge, split a single bridge into multiple, virtual bridges. When split this way, broadcasts, instead of going to all ports, get limited to only those ports associated with the virtual bridge, and its virtual LAN.

Limiting broadcasts to a VLAN does not seem by itself to prevent a system on one VLAN from hopping to another VLAN-- that is, contacting a system on the same bridge, but a different VLAN. But remember that broadcasts get used to acquire the MAC address that is associated with a particular IP address, using ARP, and without the MAC address, one system cannot communicate with another on the same network. Routers, or switches that support layer three, support passing traffic between VLANs.

Over time, people have begun to consider switches as security devices rather than networking devices. Switches do make sniffing traffic destined for other systems more difficult (but not impossible, as exploits exist for doing so). And switches do produce a software-based isolation between VLANs. But that isolation is imperfect at best.

In a document found on the Cisco web site, two scenarios are described where packets can hop VLANs, that is, pass between two VLANs on the same switch. In the first example, systems have established TCP/IP communications on the same VLAN, then the switch gets configured so that one system's port now belongs to a different VLAN. Communications continues between the two systems because each has the MAC address of the other in its ARP cache, and the bridge knows which destination MAC address gets directed to which port. In the second example, someone wishing to hop VLANs manually enters a static ARP entry for the desired system. Doing so requires that the person somehow learns the MAC address of the target system, perhaps through physical access to the target system.

Each of these two examples can be blocked by using switch software that removes the information necessary for passing packets between VLANs. In higher end Cisco switches, separate spanning trees, the tables that map MAC addresses to ports, exist for each VLAN. Other switches either have similar features, or can use configuration to filter the bridging information available to members of each VLAN.

Given the relative dearth of information about hopping VLANs within a single switch, this issue does not appear to be a serious problem.

UNITÀ DI APPRENDIMENTO

3

Tecniche crittografiche per la protezione dei dati

L1 **La crittografia simmetrica**
L2 **La crittografia asimmetrica**
L3 **Certificati e firma digitale**

Esercitazioni di laboratorio

1 L'algoritmo di cifratura RSA in C++; 2 Un algoritmo di cifratura con PHP: MD5; 3 La crittografia in PHP: form sicuro con crypt(); 4 Crittografia in PHP con algoritmo Blowfish; 5 Creazione di volumi criptati con VeraCrypt; 6 La firma digitale con la carta CNS-TS; 7 Algoritmi di cifratura in C++

Conoscenze

- Conoscere il significato di cifratura
- Avere il concetto di chiave pubblica e privata
- Riconoscere le tecniche monoalfabetiche per trasposizione e sostituzione
- Distinguere le tecniche polialfabetiche di Alberti e Vigenere
- Apprendere i metodi poligrafici e i nomenclatori
- Conoscere la crittografia a chiave simmetrica e pubblica
- Individuare i campi di applicazione delle firma digitale
- Conoscere la struttura dell'algoritmo MD5

Competenze

- Saper distinguere tra i cifrari DES, 3-DES e IDEA
- Conoscere l'algoritmo RSA
- Utilizzare le funzioni crittografiche in PHP
- Criptare file e volumi con VeraCrypt
- Conoscere i possibili utilizzi della firma digitale

Abilità

- Realizzare algoritmi di cifratura (Blowfish, RSA, MD5)
- Applicare la firma digitale alla carta CNS
- Applicare i certificati digitali

AREA *digitale*

- Esercizi
- *New directions in Cryptography*, articolo completo

Soluzioni
Puoi scaricare il file anche da hoepliscuola.it

LEZIONE 1

La crittografia simmetrica

In questa lezione impareremo...

- il significato di cifratura
- il concetto di chiave pubblica e privata
- la crittografia elettronica a chiave simmetrica
- il cifrario DES e IDEA

La sicurezza nelle reti

Il problema della sicurezza nelle reti riveste una grande importanza dato che le reti per loro natura non sono sicure: basta un ◀ analizzatore di rete ▶ come un semplice *packet sniffer* tipo wireshark per intercettare le informazioni che viaggiano su di essa.

◀ Un analizzatore di rete è un programma che permette di esaminare il traffico tra due stazioni qualsiasi della rete. ▶

L'utilizzo della rete come strumento di transazioni commerciali, e quindi come mezzo di "trasferimento di denaro", ha incontrato come ostacolo alla piena diffusione la non completa fiducia da parte degli utenti di Internet verso gli strumenti telematici per comunicare i propri dati segreti per l'accesso ai conti correnti o per l'utilizzo di carte di credito online.
In relazione alla diffusione di documenti e transazioni commerciali in rete, possiamo individuare diversi aspetti connessi al *problema della sicurezza*:

- la segretezza;
- l'autenticazione;
- l'affidabilità dei documenti.

Con segretezza si intende l'aspetto più classico cioè che le informazioni siano leggibili e comprensibili solo a chi ne ha i diritti, cioè solo alle persone autorizzate: è necessario che gli altri non le possano intercettare o, comunque, non siano in grado di comprenderle.

Con autenticazione si intende il processo di riconoscimento delle credenziali dell'utente in modo di assicurarsi dell'identità di chi invia messaggi o esegue operazioni evitando che qualche malintenzionato si spacci per qualcun altro.

Con l'affidabilità dei documenti si intende di avere la garanzia e la certezza che un documento sia originale, cioè che il suo mittente sia certo (ad esempio mediante l'apposizione su di esso di una firma digitale) e che non sia stato letto e/o alterato e modificato da altre persone non autorizzate.

Le misure da intraprendere per ottenere la segretezza possono essere anche affrontate in diversi livelli della pila protocollare: a livello fisico si può cercare di impedire che avvengano intercettazioni di dati, a livello di data link si possono introdurre codifiche dei dati trasmessi per renderli incomprensibili agli hacker.
È comunque il livello di applicazione che può gestire gli altri due problemi ed è su quello che noi concentreremo la nostra attenzione.

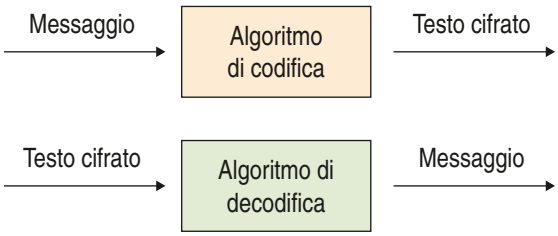
Possiamo riassumere in due aspetti le richieste degli utenti di Internet:
- **A** la possibilità di codificare i dati scambiati per renderli incomprensibili;
- **B** la garanzia di integrità e autenticazione del mittente.

Entrambi hanno come base la ◀ crittografia ▶.

◀ La crittografia rappresenta l'insieme delle tecniche che consentono di realizzare la cifratura di un testo e la decifratura di un crittogramma. ▶

Crittografia

Il desiderio di mantenere nascosti messaggi tra due interlocutori agli occhi di terzi non è una necessità nata con Internet; possiamo trovare tracce di tentativi di occultamento delle informazioni già su geroglifici di 4500 anni fa.
La cifratura rappresenta il processo attraverso il quale un messaggio viene reso incomprensibile per gli estranei. Per fare questo viene usato un algoritmo di cifratura che stabilisce una corrispondenza tra i simboli in chiaro e simboli cifrati: i simboli in chiaro vengono utilizzati per creare il messaggio in chiaro (plain text) che, una volta cifrato, diviene un testo criptato (cipher text).
Le regole di cifratura devono essere note sia al mittente del messaggio che al destinatario, in modo che quest'ultimo possa, alla sua ricezione, effettuarne il decriptaggio e comprenderne il significato.



Gli esperti di crittografia utilizzano anche il termine codifica, attribuendogli un significato diverso da quello degli informatici: con codifica essi intendono un "metodo di scrittura in chiave che consiste nel sostituire alcune parole con altre" distinguendolo dalla cifratura che più precisamente "sostituisce lettere o caratteri".

ESEMPIO

Se volessimo trasferire una parola come "AIUTO" utilizzando i due metodi potremmo:
- **A** trasmettere "HELP" oppure "SOCCORSO", cioè sostituire completamente la parola con un'altra, magari in una lingua diversa, non conosciuta a chi potrebbe intercettarla (codifica); la lingua degli Indiani Navajo fu usata nella II guerra mondiale per le operazioni nel Pacifico;
- **B** trasmettere "BLVUP", cioè sostiture a ciascuna lettera quella che la segue nell'alfabeto (cifratura).

Quest'ultimo esempio ci permette di effettuare una osservazione: la regola di cifratura è generalmente composta da due elementi:

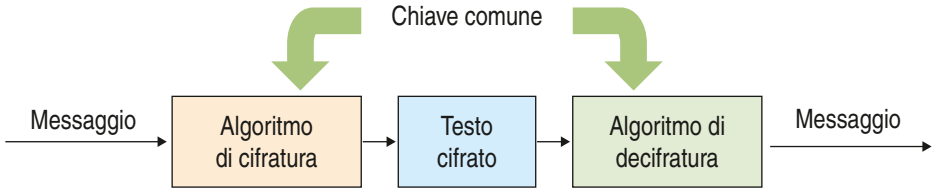
A la regola vera e propria (l'algoritmo utilizzato), che in questo caso consiste nella "sostituzione di un carattere con un altro";

B uno (o più) parametri, in questo caso la posizione del carattere da prendere (nell'esempio il successivo a quello in chiaro: se invece si fosse trasmesso CMZVQ le posizioni sarebbero state due in avanti).

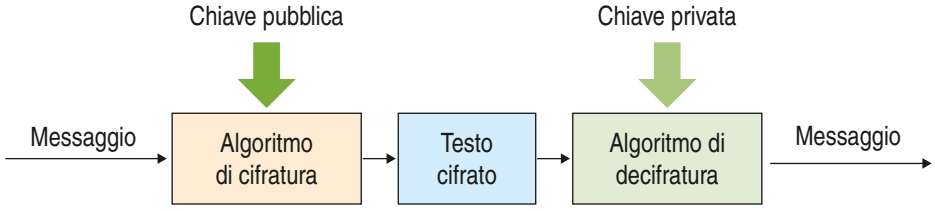
La distinzione tra regola e parametro è fondamentale nella crittografia: l'hacker deve conoscerli sempre entrambi e, quindi, basta modificarne uno periodicamente o in base ad accordi prestabiliti per aumentare la complessità di intercettazione.

La *regola* prende il nome di algoritmo di criptazione mentre il *parametro* di chiave.

Quando la chiave di cifratura coincide con quella di decifratura lo schema crittografico si dice simmetrico e la chiave prende il nome di chiave comune.



Quando la chiave di cifratura è invece diversa da quella usata per la decifratura lo schema crittografico si dice asimmetrico e le due chiavi si chiamano chiave pubblica quella usata per la cifratura, che è comune a tutti i mittenti e di pubblico dominio, e chiave privata quella utilizzata per la decifratura, che è segreta e di conoscenza solo del destinatario del messaggio.



Questo procedimento è alla base della moderna sicurezza delle reti: il mittente non deve comunicare col destinatario o accordarsi preventivamente, ma utilizza la chiave pubblica del destinatario che, proprio perché pubblica, è a disposizione di tutti, e con essa prepara il messaggio da trasmettere criptandolo in modo tale che solo chi è in possesso della chiave privata lo può decriptare.

È necessario che chiave pubblica e chiave privata siano *diverse*: per migliaia di anni la possibilità di cifrare un messaggio con una chiave e decifrarlo con una seconda chiave diversa dalla prima sembrava un assurdo, ma oggi, come vedremo in seguito, questo è possibile ed è utilizzato regolarmente nella pratica giornaliera.

Crittoanalisi

◀ Crittoanalisi La parola crittoanalisi proviene dal greco κρυπτός ("kryptós"= nascosto) αναλύειν ("analùein" = scomporre) e comporta lo studio dei metodi per ottenere il significato di informazioni cifrate: tipicamente si tratta delle operazioni effettuate alla ricerca della chiave segreta. ▶

Generalmente l'algoritmo di cifratura è noto e standardizzato, quindi conosciuto e soggetto a ◀ crittoanalisi ▶ da parte dei malintenzionati per individuare la chiave utilizzata e quindi decriptare il messaggio.

◀ L'attacco di un crittoanalista mirato a violare (rompere, sfondare) il crittosistema prende il nome di crittoanalisi. ▶

Per poter effettuare un ◀ attacco ▶ gli intrusi devono essere in possesso dei messaggi cifrati e la natura stessa di Internet rende questa operazione molto semplice: lo scopo della crittografia è quello di rendere difficile la decifrazione del messaggio.

Il principio di Kerckhoffs (1835-1903) stabilisce che è la chiave l'elemento fondamentale per la sicurezza di un sistema informatico: la sicurezza di un crittosistema deve dipendere solo dalla segretezza della chiave e non dalla segretezza dell'algoritmo usato.
Come corollario al principio, Shannon aggiunse la frase: «il nemico conosce il sistema».

A partire dal principio di Kerckhoffs si sono nel tempo aggiunte alcune riflessioni che hanno avuto un ruolo fondamentale nella moderna crittografia: le chiavi sono generalmente semplici e possono essere cambiate più frequentemente dell'algoritmo quindi, una volta determinato un buon algoritmo, è sufficiente "concentrarsi" sulla loro gestione.
Si è anche arrivati alla definizione di un cifrario assolutamente sicuro, il cosiddetto one-time pad: in esso le due parti in comunicazione condividono un blocco (pad) di chiavi di sostituzione alfabetica generate con un procedimento casuale, e *cambiano la chiave a ogni lettera*.

One-time pad

Se il messaggio viene intercettato l'intruso vede solamente una sequenza di caratteri casuali e non è in grado di decifrare il messaggio.
Questo meccanismo trova implementazione nel cifrario di Vernam che descriveremo in seguito che, come dimostrato da Shannon, richiede per la sua realizzazione una chiave lunga quanto il messaggio stesso e necessita che il mittente e il destinatario siano sincronizzati per essere sicuri di partire dalla stessa posizione del blocco: risulta inoltre complesso realizzare il blocco chiave in modo che sia anch'esso sicuro.

Oggi esistono dei sistemi che generano e utilizzano una password usa e getta, soprattutto per transazioni bancarie, che possiamo dire ispirati al one-time pad: possono definirsi sistemi one-time key (OTK) in quanto la chiave può essere utilizzata una sola volta dato che generalmente ha una validità temporale modesta (10-20 secondi) dopo che è generata da un dispositivo elettronico (key generator) che è sincronizzato con il sistema di controllo di accesso al servizio.

One-time key

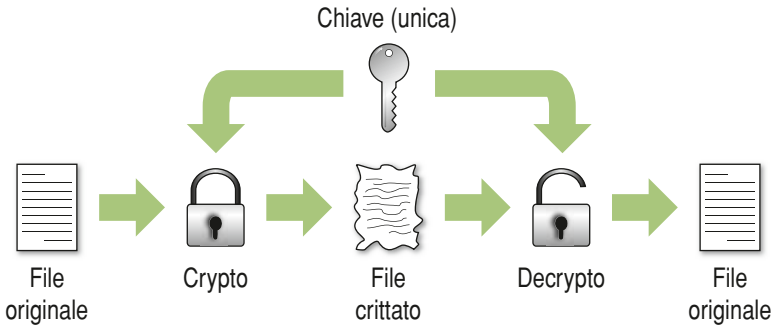
Cifrari e chiavi

Oltre a garantire la segretezza dei messaggi, la crittografia consente di:
- identificare un utente all'accesso alla rete o al singolo PC;
- autenticare un messaggio, cioè accertarsi dell'identità dell'autore e della integrità del messaggio ricevuto;
- firmare digitalmente un messaggio, in modo da permettere la verifica dell'autore e quindi la non ripudiabilità del messaggio stesso.

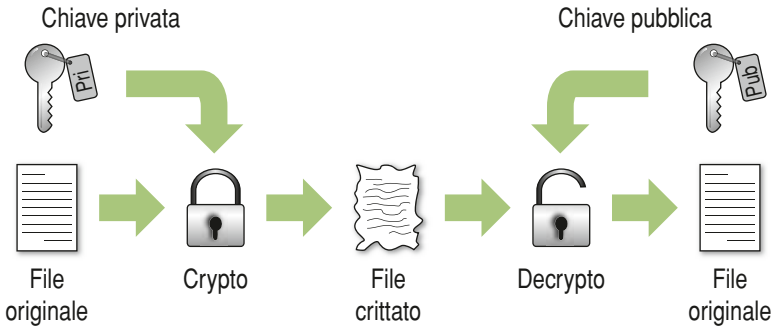
Tutti i cifrari tradizionali sono caratterizzati da una (o più) chiave segreta che mittente e destinatario dei messaggi segreti devono concordare e quindi scambiarsi prima di poter comunicare: questa

esigenza è un grosso punto debole in quanto è praticamente impossibile avere un canale sicuro. I sistemi crittografici contemporanei vengono classificati proprio in base al tipo e al numero di chiavi usate:

- sistemi a chiave simmetrica (o privata): viene utilizzata una sola chiave:



- sistemi a chiave asimmetrica (o pubblica): sistemi dove ogni utente dispone di due chiavi, una pubblica e una privata (le chiavi sono invertibili):



Il cifrario DES

Uno dei primi sistemi crittografici moderni a chiave simmetrica è stato sviluppato da Horst Feistel per l'IBM nel 1976 ed è diventato uno standard negli USA per la protezione di dati sensibili.

La National Security Agency (USA) e il National Bureau of Standards (USA) lo ritenne un sistema pubblico, efficiente, compatibile e venne quindi certificato.

DES è un algoritmo simmetrico a chiave segreta di 64 bit ma dei quali 8 sono di controllo, quindi solo 56 bit utili, e tramite questa chiave prevede 16 trasformazioni successive applicate a ogni blocco del messaggio.

> Le trasformazioni sono sia di trasposizione che di sostituzione, quindi il DES è un cifrario misto.

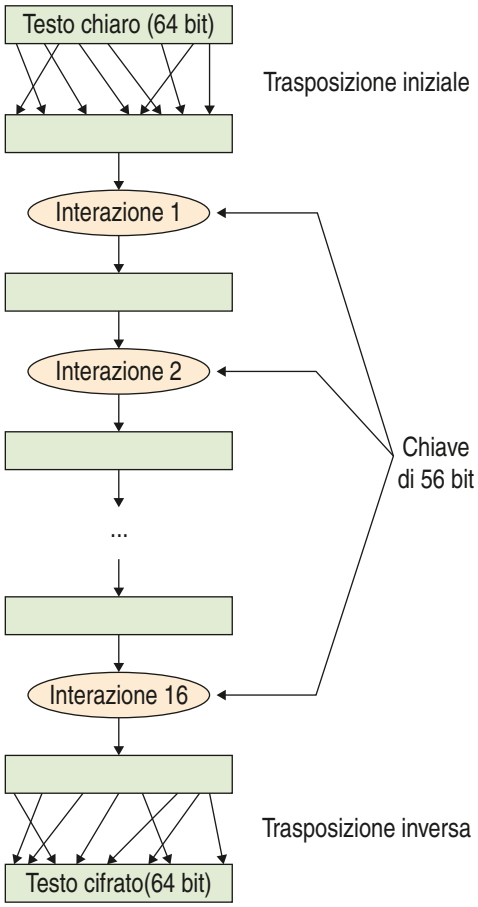
Ricordiamo che nei computer la crittografia deve lavorare non più su di un alfabeto di 26 lettere ma su file binari con byte codificati in ASCII, quindi con 128 caratteri di cui solo 96 sono i cosiddetti printable characters.

Il DES rispetta il principio di Kerckhoffs, cioè l'algoritmo è noto ed è la chiave segreta, ed è stato realizzato applicando i principi di Shannon:

- diffusione dei caratteri consecutivi del messaggio in tutto il crittogramma;
- confusione del messaggio con la chiave.

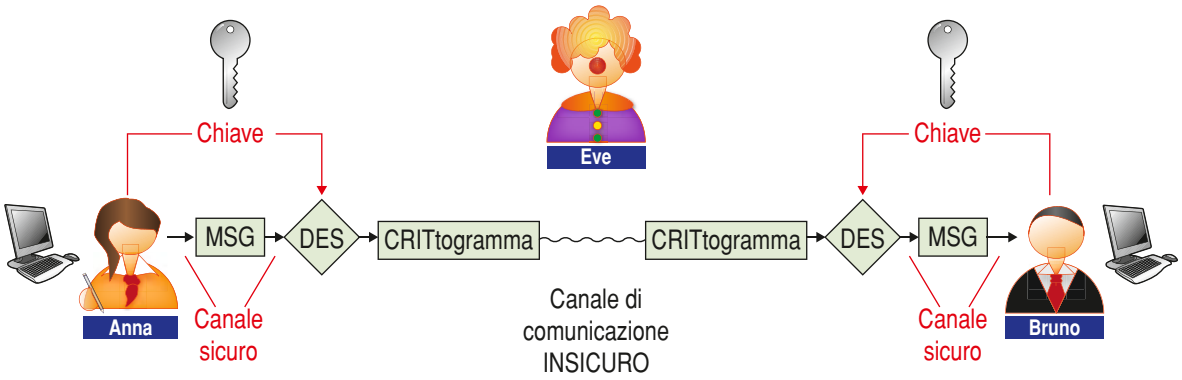
Praticamente il testo in chiaro viene suddiviso in blocchi di 8 byte e scrivendo la codifica ASCII da ogni blocco si otterrà una stringa di 64 cifre binarie: a queste cifre viene applicata una trasposizione di 56 bit alla chiave e successivamente per 16 volte si applica una funzione cifrante di sostituzione

dei bit, usando due porzioni della chiave di 28 bit ciascuna delle quali viene ruotata a sinistra di un certo numero di bit che dipende dal numero di iterazione; come ultimo passaggio viene effettuata una trasposizione inversa a quella iniziale. Il funzionamento è sintetizzato nello schema seguente:



La decifrazione avviene utilizzando la medesima chiave adoperata per la cifratura, solo che i passi vengono effettuati nell'ordine inverso: è quindi un sistema simmetrico dato che sia l'emittente del messaggio che il ricevente devono conoscere la stessa chiave segreta.

Una caratteristica desiderata per ogni algoritmo di criptazione è quello che prende il nome di effetto valanga: un cambiamento di pochi bit nel plaintext deve provocare un cambiamento di quanti più bit nel ciphertext, e il DES possiede un forte effetto valanga.



Il DES viene anche utilizzato per cifrare file personali su di un disco locale.

Per circa vent'anni il DES è stato utilizzato come un cifrario assolutamente sicuro e alla sua presentazione fu comunicato che per violarlo esaustivamente sarebbe stato necessario costruire un elaboratore dal costo stimato in un 1 milione di dollari.
Le prime critiche arrivarono verso al fine del secolo scorso, soprattutto per la lunghezza della chiave ritenuta insufficiente: le chiavi possibili sono 2^{56} che, pur essendo un numero molto elevato, doveva "competere" con l'evoluzione tecnologica dei moderni supercomputer.

DES FU VIOLATO NEL '98

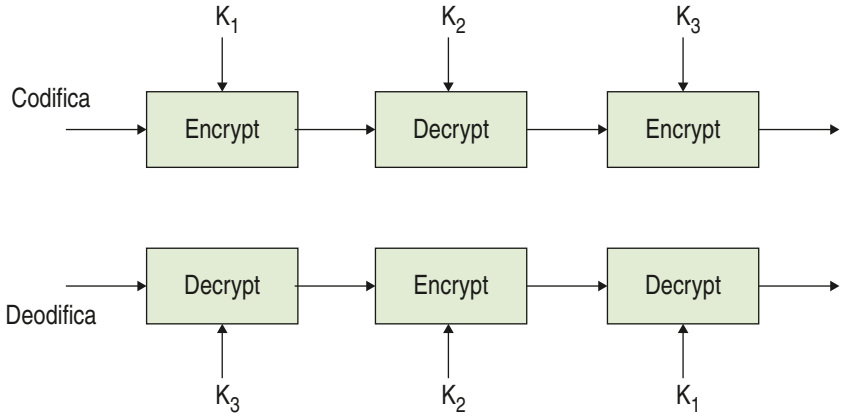
Il 17 luglio 1998 la Electronic Frontier Foundation diffuse un comunicato stampa con il quale annunciò la definitiva sconfitta del DES effettuata grazie a un calcolatore costato 250.000 dollari che in meno di sessanta ore era capace di forzare un messaggio cifrato con DES.

La relativa vulnerabilità dell'algoritmo DES ha comportato lo studio di nuove tecniche e di un nuovo algoritmo: dapprima si realizzò, nel 1999, il Triple Des basandosi sullo stesso algoritmo ma utilizzando chiavi più lunghe e più passaggi di cifratura; successivamente, nel 2001, venne pubblicato un nuovo standard di sostituzione, l'AES Advanced (Encryption Standard).

Nonostante tutto, oggi il DES rimane ancora ampiamente utilizzato.

3-DES

Nel 1999 è stato introdotto Triple DES, con tre passi di cifratura DES consecutivi con tre chiavi diverse e per un totale di 168 bit: la maggior sicurezza rispetto al sicurezza al DES è proprio nella lunghezza tripla della chiave.
Codifica e decodifica avvengono secondo il seguente schema:



Il passo centrale, come si può vedere dalla figura, è in realtà una decifrazione, cioè è "applicato al contrario".

In base alla scelta delle chiavi il sistema 3DES offre tre alternative:
1. le tre chiavi K1, K2 e K3 sono diverse e indipendenti;
2. due chiavi uguali K1 = K3 e una diversa (K2);
3. le tre uguali K1 = K2 = K3.

Con la seconda opzione, avendo solo due chiavi da 56 bit, la sicurezza è a 112 bit.
La terza opzione viene usata esclusivamente per garantire la compatibilità con DES: i primi due passi si annullano, per cui l'applicazione di 3DES con keying option 3 è equivalente a quella di DES normale e quindi la sicurezza della chiave è 56 bit, come DES.

Oggi il sistema 3DES viene utilizzato con alcune varianti nelle transazioni commerciali elettroniche (circuiti VISA, Mastercard ecc).

IDEA

Nel 1991 fu proposto il cifrario IDEA (International Data Encryption Algorithm) in sostituzione del DES, proprio quando si temeva che questo non sarebbe ancora resistito per molto agli attacchi degli analisti.
Il metodo progettato in Svizzera a opera dei due famosi ricercatori Xuejja Lai e James L. Massey si basa su concetti simili al DES con chiave a 128 bit dove i blocchi di 64 bit del messaggio vengono elaborati in 8 iterazioni usando le operazioni di XOR, di somma e moltiplicazione modulo 216.

I 64 bit del messaggio vengono divisi in 4 gruppi di 16 e mescolati con 6 chiavi di 16 estratte dalla chiave di 128 bit.
Le sottochiavi sono generate in questo modo:

- la chiave a 128 bit è divisa in 8 blocchi di 16 che costituiscono le prime 8 sottochiavi;
- le cifre della chiave a 128 sono spostate di 25 bit a sinistra in modo da generare una nuova combinazione, il cui raggruppamento a 8 bit fornisce le prossime 8 sottochiavi;
- il secondo passo è ripetuto finché le 52 sottochiavi sono generate.

Durante gli 8 passi il secondo e il terzo blocco si scambiano di posto mentre all'ultimo passo i 4 sottoblocchi vengono concatenati per produrre un blocco di testo cifrato a 64 bit.

Attualmente non si conoscono tecniche in grado di forzare IDEA che, grazie alla chiave a 128 bit, è immune ad attacchi "brutali" ed *è il cifrario a chiave segreta più utilizzato* per quanto riguarda i software commerciali di crittografia vista la sua velocità di codifica e decodifica e la sua elevata sicurezza.

AES

Nel 1997 il NIST (National Institute of Standards and Technology) USA organizzò un "concorso" per sostituire l'ormai insicuro DES e definire un nuovo standard crittografico, l'Advanced Encryption Standard (AES). Si presentarono 15 candidati con proposte di nuovi algoritmi e soluzioni criptografiche: dopo lunghi test e rigorose analisi nel 2000 vinse l'algoritmo Rijndael, proposto da due crittologi belgi, che divenne ufficialmente il nuovo standard, grazie alle sua velocità di esecuzione e alle caratteristiche di robustezza alla crittanalisi.

Metodi di valutazione di AES

La valutazione degli algoritmi che parteciparono al concorso furono effettuati dal NIST secondo due diversi metri di giudizio.
La prima valutazione si basò sulla verifica di requisiti fondamentali:

- sicurezza: dato che in AES la chiave ha dimensioni minime di 128 bit, gli attacchi a "forza bruta" (brute force) con le tecnologie attuali e future non vennero neppure considerati;
- costo: dato che la richiesta del NIST fu quella di un algoritmo da poter essere impiegato per un'ampia gamma di applicazioni, doveva avere un'elevata efficienza computazionale e doveva poter essere utilizzato nei collegamenti a banda larga;
- caratteristiche dell'algoritmo e dell'implementazione: per questi requisiti si richiedevano vari aspetti progettuali dell'algoritmo, tra cui la leggibilità, la semplicità di codifica, la flessibilità e versatilità per poter essere implementato in differenti piattaforme hardware e software.

Tra tutti i progetti, cinque furono selezionati come finalisti e si analizzarono più dettagliatamente i seguenti aspetti:

- sicurezza generale: furono resi pubblici gli algoritmi e vennero valutati dalla comunità crittografica;
- implementazioni software: fu valutata la velocità di esecuzione in diverse piattaforme hardware e con diversi sistemi operativi, anche in funzione della variazione della dimensione della chiave;
- ambienti con spazio limitato: tra gli obiettivi c'era quello di poter implementare ed eseguire l'algoritmo anche in situazioni di risorse limitate, come ad esempio con le Smart Card;
- crittografia e decrittografia: analisi e comparazione delle risorse richieste tra la fase di crittografia e quella decrittografia nel caso in cui i due algoritmi siano separati e quindi richiedano maggiore spazio di memoria;
- agilità della chiave: intesa come la capacità, la rapidità e il costo necessario per effettuare il cambiamento della chiave;
- versatilità e flessibilità: possibilità di utilizzare blocchi e chiavi di dimensioni diverse;
- potenzialità di sfruttamento del parallelismo: capacità di sfruttare le architetture parallele e quindi di poter avere esecuzione contemporanea a livello delle istruzioni per massimizzare l'efficienza del sistema.

L'algoritmo Rijndael risultò vincitore e successivamente approvato dal Segretario del Dipartimento di Commercio americano: rispetta praticamente tutti i canoni richiesti dal NIST ed è resistente a tutti gli attacchi a un costo computazionale relativamente molto basso.

L'algoritmo AES

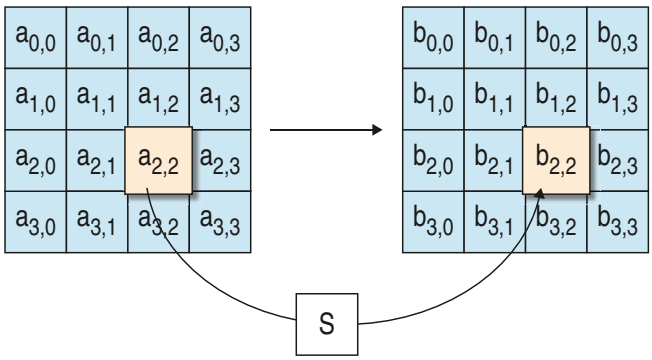
AES fu progettato dai due crittologi Joan Daemen e Vincent Rijmen sulla base di tre caratteristiche fondamentali:

- resistenza contro tutti gli attacchi;
- velocità e compattezza del codice su un'ampia gamma di piattaforme;
- semplicità progettuale.

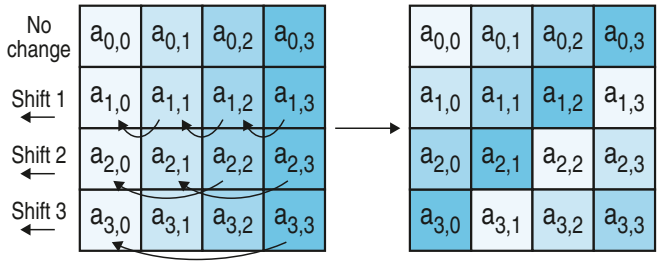
AES è un cifrario a blocchi (block cipher) con lunghezza del blocco da 128 bit, ma può avere chiavi indipendenti l'una dall'altra con lunghezza variabile di 128, 192 o 256 bit, ed effettua una combinazione di permutazioni e sostituzioni.

> In pratica viene utilizzata maggiormente la chiave di lunghezza 128 bit.

La prima operazione eseguita dall'algoritmo è quella di prendere i 128 bit del blocco (16 caratteri) e di disporli in una griglia di 4 × 4 byte: si procede quindi con la codifica, che consiste fondamentalmente in un insieme di 10 fasi (rounds) ciascuna composta da 4 trasformazioni (nel caso di chiavi a 128 bit).
Le quattro operazioni che costituiscono ogni round sono le seguenti:

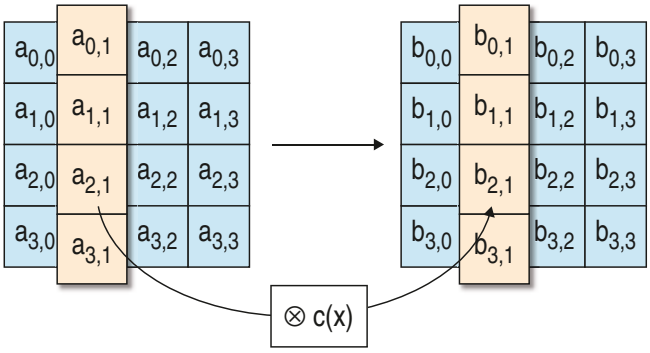


Substitute Bytes: ogni byte viene trasformato mediante una permutazione non lineare di byte che vengono mappati tramite una tabella particolare definita in AES stesso (tabella S-box in figura).

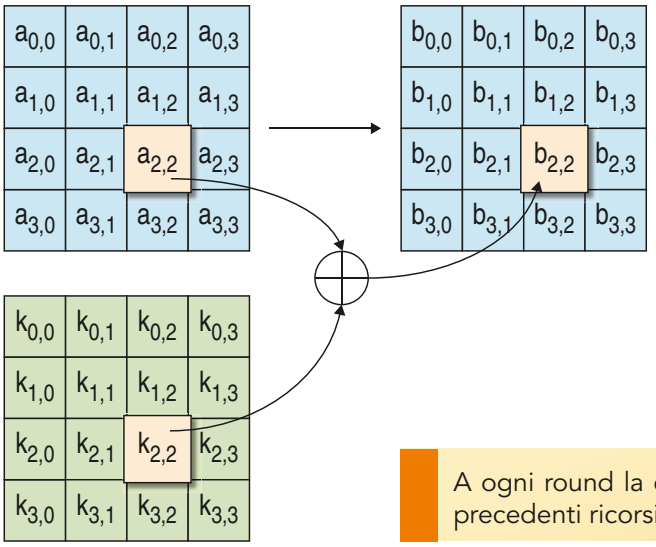


Shift Rows: le righe della matrice subiscono un semplice scorrimento di bytes nell'array ◀ **state** ▶, dove la prima riga rimane invariata, dalla seconda alla quarta viene sempre eseguito uno scorrimento circolare a sinistra di uno, due e tre bytes rispettivamente.

◀ Il risultato intermedio delle operazioni fatte durante l'algoritmo prende il nome di state, rappresentabile come un array di bytes. ▶



Mix Columns: ogni colonna viene trasformata mediante una operazione che può essere vista come una moltiplicazione matriciale con una particolare matrice generata da un polinomio prefissato.



Add Round Key: questa non è altro che la fase in cui viene inserita la chiave segreta che rende il cifrario sicuro: ogni byte viene combinato in XOR con la chiave da 128 bit (16 bytes).

A ogni round la chiave aggiunta è diversa e ricavata dalle precedenti ricorsivamente.

Il NIST si pronunciò così sull'algoritmo Rijndael:

> Non esiste alcun attacco noto alla sicurezza di Rijndael. Rijndael utilizza una S-box come componente non lineare. Rijndael sembra avere un margine di sicurezza adeguato, ma ha ricevuto qualche critica che suggerisce che la sua struttura matematica potrebbe essere soggetta ad attacchi. D'altro canto, la semplicità della sua struttura dovrebbe aver facilitato l'analisi della sicurezza durante il processo di sviluppo dello standard AES.

AES è il primo standard approvato da NSA (National Security Agency) per comunicazioni top-secret ed è tuttora il cifrario a chiave segreta più usato negli ambienti informatici: a oggi non sono conosciuti attacchi in grado di violarlo (né di crittoanalisi lineare né differenziale) e l'unico che forse potrebbe farlo (The Square attack) impiegherebbe tempi inaccettabili.

DES e AES sono utilizzati per la validazione di *password* segrete (identificazione dell'utente).

Limiti degli algoritmi simmetrici

Gli algoritmi simmetrici descritti presentano alcuni limiti tra i quali il problema più evidente è quello che nella crittografia simmetrica le persone che devono comunicare devono essere in possesso della stessa chiave e, di fatto, questo limita la diffusione e il suo utilizzo, in quanto non sono molti i sistemi a disposizione per la distribuzione delle chiavi.

ESEMPIO

Se si vuole utilizzare la crittografia simmetrica per effettuare acquisti online bisogna richiedere al gestore della transazione una chiave per poter codificare i dati, ma come verrebbe codificato il messaggio contenente la chiave?

L'idea di utilizzare corrieri fidati resta nella maggior parte delle situazioni impraticabile, soprattutto con l'aumentare degli utenti: inoltre è inutilizzabile in campo militare in quanto è "difficile" far pervenire la chiave durante le missioni!
Non è inoltre percorribile la strada di inviare la chiave per posta elettronica, neanche scomponendola in parti e ricomponendola secondo un criterio concordato, poiché "anch'esso deve essere comunicato".

Inoltre l'utilizzo continuato della medesima chiave potrebbe favorire azioni di decriptaggio così come l'evoluzione tecnologica che potrebbe portare alla realizzazione di computer talmente veloci da essere in grado di violare questi sistemi che, come abbiamo visto, sono realizzati con un insieme di operazioni semplici (trasposizione e sostituzione).
In ultimo il destinatario potrebbe perdere o cedere ad altri la propria chiave, con i danni che possiamo immaginare.

Questi limiti sono superati con la crittogafia asimmetrica, dove non è necessario concordare le chiavi di cifratura.

Verifichiamo le conoscenze

1. Risposta multipla

1 La chiave pubblica è:

a. usata per la cifratura nello schema crittografico simmetrico
b. usata per la decifratura nello schema crittografico simmetrico
c. usata per la cifratura nello schema crittografico asimmetrico
d. usata per la decifratura nello schema crittografico asimmetrico

2 La chiave privata è:

a. usata per la cifratura nello schema crittografico simmetrico
b. usata per la decifratura nello schema crittografico simmetrico
c. usata per la cifratura nello schema crittografico asimmetrico
d. usata per la decifratura nello schema crittografico asimmetrico

3 La chiave comune è: (2 risposte)

a. usata per la cifratura nello schema crittografico simmetrico
b. usata per la decifratura nello schema crittografico simmetrico
c. usata per la cifratura nello schema crittografico asimmetrico
d. usata per la decifratura nello schema crittografico asimmetrico

4 L'algoritmo DES (indica le affermazioni errate):

a. è un algoritmo simmetrico
b. è un cifrario misto
c. ha chiave segreta di 64 bit
d. 16 bit della chiave sono di controllo
e. prevede 16 trasformazioni successive

5 In base alla scelta delle chiavi il sistema 3DES offre tre alternative (indica quelle errate):

a. le tre chiavi K1, K2 e K3 sono diverse
b. due chiavi uguali K1 = K3
c. due chiavi uguali K1 = K2
d. due chiavi uguali K2 = K3 e una diversa
e. tre chiavi uguali K1 = K2 = K3

6 Cosa significa l'acronimo IDEA?

a. Internal Data Encryption Asimmetric
b. Internal Data Encryption Algorithm
c. International Data Encryption Algorithm
d. International Data Encryption Asimmetric

7 AES fu valutato in base a:

a. sicurezza
b. costo
c. lunghezza delle chiavi
d. caratteristiche dell'algoritmo e dell'implementazione

8 AES fu progettato sulla base di tre caratteristiche fondamentali:

a. resistenza contro tutti gli attacchi
b. costo
c. velocità e compattezza del codice su un'ampia gamma di piattaforme
d. semplicità progettuale

2. Ordinamento

1 Ordina le quattro operazioni che costituiscono ogni round del AES:

a. ..... Mix Columns
b. ..... Shift Rows
c. ..... Add Round Key
d. ..... Substitute Bytes

3. Vero o falso

1 Nei sistemi a chiave simmetrica la chiave del mittente è simmetrica a quella del destinatario. V F
2 Nei sistemi a chiave asimmetrica sono necessarie due chiavi, una pubblica e una privata. V F
3 In base alla scelta delle chiavi il sistema 3DES offre tre alternative. V F
4 AES è un cifrario a blocchi (block cipher) con lunghezza del blocco da 128 bit. V F
5 AES è un cifrario a blocchi con chiave di 128 bit. V F
6 Nell'AES vengono effettuati 10 state. V F

LEZIONE 2

La crittografia asimmetrica

In questa lezione impareremo...

- il meccanismo a chiave pubblica
- l'algoritmo RSA
- la crittografia ibrida

Generalità

La crittografia simmetrica a chiave privata non è il metodo crittografico ideale per le comunicazioni e le transazioni su Internet: il limite fondamentale è rappresentato dalla necessità di un canale sicuro e di un accordo preventivo per lo scambio delle chiavi e questo non è funzionale nei casi in cui è necessario stabilire connessioni sicure estemporanee.

> La crittografia a chiave pubblica nacque nel maggio del 1975, come conseguenza di due problemi… il problema della distribuzione delle chiavi e quello delle firme elettroniche… La scoperta non consisteva in una soluzione, ma nel capire che i due problemi, ognuno dei quali sembrava irrisolvibile per definizione, poteva essere risolto e che la soluzione di entrambi scaturiva da un solo metodo.
>
> Whitfield Diffie e Martin E. Hellman, *New directions in Cryptography* (1976).

AREA *digitale*

New directions in Cryptography, articolo completo

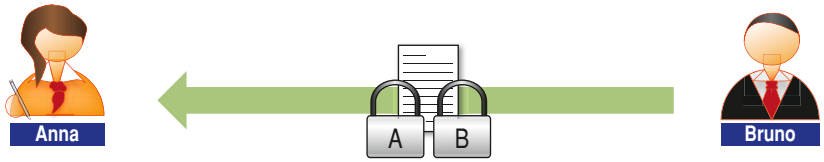
L'idea alla base delle crittografia asimmetrica è quello di avere due chiavi diverse, una pubblica per la criptazione e una privata per la decriptazione, che deve essere mantenuta segreta.
In questo caso non è necessario lo scambio delle chiavi, che per la maggior parte saranno pubbliche.

ESEMPIO

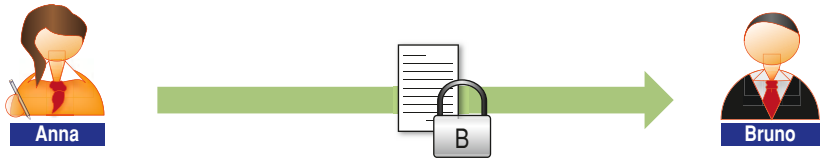
Vediamo il funzionamento mediante un esempio che pone sul messaggio "fisicamente" una chiave mediante un lucchetto:

1. Anna manda a Bruno il messaggio in una scatola chiusa con un suo lucchetto A: né Bruno né gli intrusi possono aprirlo;

2 Bruno lo rispedisce ad Anna aggiungendo un suo lucchetto B: nessuno ora è in grado di aprirlo;

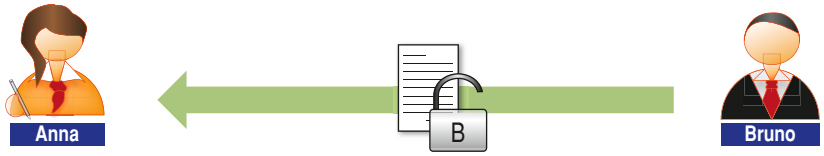


3 Anna toglie il suo lucchetto e rimanda il pacco a Bruno, che ora ha solo il suo lucchetto e che alla sua ricezione può aprirlo e leggere il messaggio.

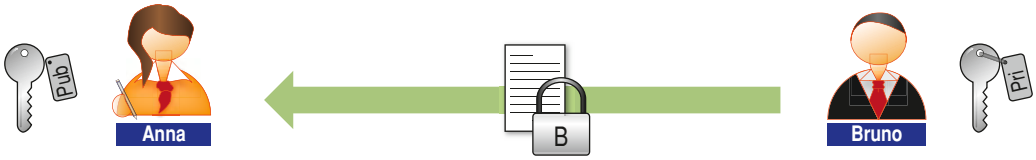


In questo caso però il messaggio deve essere trasmesso tre volte con enorme dispendio di risorse: un' idea migliore è quella descritta di seguito, dove viene inviato il "lucchetto" e non il messaggio:

1 Bruno manda ad Anna il proprio lucchetto aperto e questa lo conserva fino a che ha necessità di spedire qualcosa a Bruno;



2 quando Anna deve spedire un messaggio a Bruno, lo chiude con il suo lucchetto e glielo invia: senza il triplo invio del messaggio ci siamo riportati nella situazione descritta in precedenza.



La chiusura del lucchetto viene effettuata con una specifica chiave pubblica che ciascun utente mette a disposizione di tutti gli altri utenti che necessitano di trametterli messaggi: la chiave privata è invece segreta, in possesso a ogni utente, che la utilizza per "aprire" il lucchetto e leggere il messaggio.

> Formalmente è necessario trovare una funzione *("il lucchetto")* la cui trasmissione su canali insicuri non comprometta l'algoritmo, che sia facile da applicare (parte pubblica che chiude il lucchetto) ma difficile da invertire (parte privata che apre il lucchetto).

Questo meccanismo è implementato negli algoritmi di crittografia simmetrica, come ad esempio nell'algoritmo RSA (dal nome dei suoi creatori Rivest, Shamir e Adleman) descritto in seguito.

Per ogni mittente è necessaria una chiave pubblica e una chiave privata, quindi in totale per n utenti sono necessarie 2 × n chiavi contro le [n(n–1)]/2 necessarie per i sistemi a chiave privata.

Numero di utenti	Numero di chiavi in un sistema a chiave pubblica	Numero di chiavi in un sistema a chiave privata
10	20	45
100	200	4.950
1.000	2.000	499.500
10.000	20.000	49.995.000
100.000	200.000	4.999.950.000
1.000.000	2.000.000	499.999.500.000

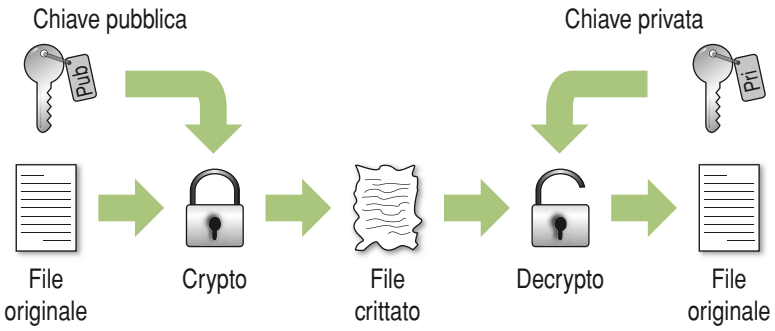
Naturalmente le due chiavi devono essere tra loro indipendenti, in modo che dalla prima non si possa in nessun modo ricavare la seconda.

Con la crittografia asimmetrica:

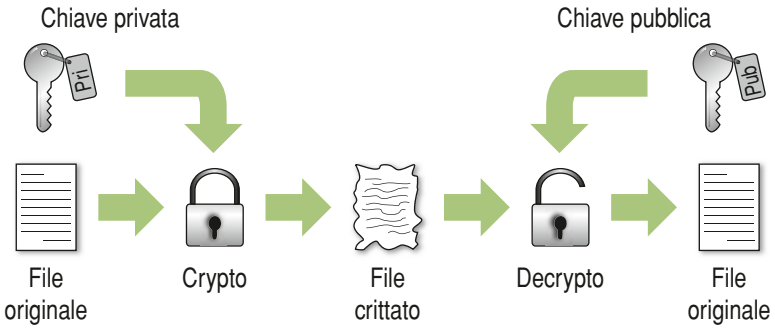
- si risolve il problema della riservatezza: criptando il messaggio con la chiave pubblica solo il possessore della chiave privata è in grado di decriptarlo;
- si risolve il problema della autenticità del mittente: criptando il messaggio con la chiave privata solo con la corrispettiva chiave pubblica questo può essere decriptato e la chiave pubblica è conservata in registri consultabili ma gestiti in modo sicuro dove a ogni chiave pubblica è associata l'identità certa del proprietario.

Abbiamo quindi due modalità di funzionamento:

1. modalità confidenziale: sono garantite la riservatezza e l'integrità del messaggio;



2. modalità autenticazione: garantisce l'integrità e il non ripudio ma non viene garantita la riservatezza (il mittente ha posto la sua firma elettronica sul messaggio).



È possibile autenticare oltre al mittente anche il contenuto del messaggio, generando un "hashing" dello stesso e aggiungendolo in fondo al messaggio: nel caso in cui ci fosse un'alterazione durante la trasmissione, alla decodifica l'hash sarebbe diverso e quindi il destinatario può accorgersi della anomalia.

ESEMPIO

Il meccanismo di funzionamento è il seguente:
Indichiamo gli utenti con le loro iniziali A, B, C,… e ogni utente ha una copia di chiavi:

- Ei: chiave pubblica per la cifratura (Encrypt), cioè EA è la chiave pubblica di A, ecc.;
- Di: chiave privata per la decifratura (Decrypt), cioè DA è la chiave privata di A, ecc.

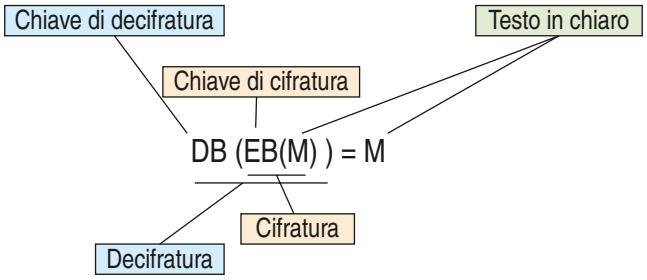
Sono quindi presenti due insiemi di chiavi: per la *funzione di codifica* EA, EB, EC,…che sono rese pubbliche e DA, DB, DC, … con *funzione segreta di decodifica*, una per ogni utente.

Supponiamo che l'utente A voglia inviare un testo in chiaro T all'utente B: questo viene diviso in blocchi e ogni blocco viene trasformato in un numero M che lo rappresenta esattamente; quindi il problema si riduce a dover cifrare i numeri M e successivamente a inviarli a B.

Messaggio cifrato per l'utente B: (EB(M))

Alla sua ricezione l'utente B applica la sua chiave privata ed effettua la decodifica del messaggio cifrato:

Messaggio decifrato dall"utente B: DB(EB(M)) = M



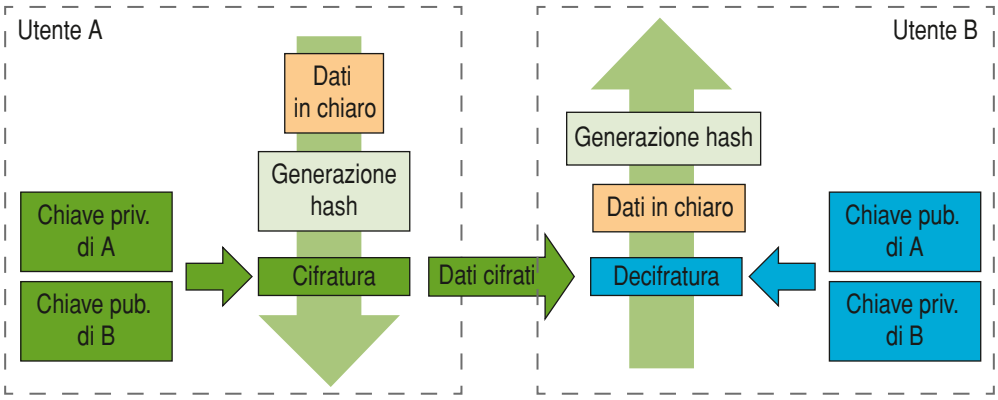
In altre parole la funzione di decodifica D è l'inverso della funzione di codifica E che però non deve essere deducibile da essa: la ricerca di una funzione con tali caratteristiche è stata la grande sfida per i crittografi degli anni '70 e un passo notevole fu fatto dai matematici Diffie e Hellman, che nel 1976 progettarono un algoritmo basato sulla aritmetica modulare (in particolare sul logaritmo discreto) in grado di permettere lo scambio delle chiavi su un canale non sicuro, di notevole importanza però più per la crittografia simmetrica che per quella asimmetrica. Fu comunque da stimolo per la ricerca in campo crittografico.

È anche possibile ottenere contemporaneamente sia la riservatezza della comunicazione che l'autenticazione combinando assieme le due modalità di funzionamento. Per fare questo è necessario utilizzare contemporaneamente entrambe le coppie di chiavi:
Anna cifra il messaggio con la chiave pubblica di Bruno e quindi solo Bruno lo può leggere; contemporaneamente firma il messaggio con la propria chiave privata: alla sua ricezione Bruno, sapendo che il mittente del messaggio è Anna, prova a decriptarlo con la chiave pubblica di Anna e, se vi riesce, può autenticare Anna come mittente, dato che solo chi è in possesso della chiave privata ha potuto cifrare il messaggio.

Si dice che "Anna ha quindi posto la sua firma elettronica sul messaggio".

Inoltre il messaggio è anche cifrato con la chiave pubblica di Bruno e quindi la trasmissione risulta inviolabile da chi non è in possesso delle chiave privata che solo Bruno detiene: è quindi garantita anche la riservatezza.

Se il messaggio prima di essere cifrato viene anche elaborato generando un hash che viene trasmesso con esso, alla sua ricezione la verifica dell'hash ci permette di scoprire se è integro oppure se è stato modificato.



Il principale svantaggio degli algoritmi a crittografia asimmetrica sta nella complessità dei calcoli che rendono poco efficiente la loro implementazione soprattutto con l'aumentare della lunghezza della chiave: gli algoritmi simmetrici e quelli asimmetrici necessitano di chiavi di lunghezze differenti per raggiungere il medesimo grado di sicurezza teorica con lunghezze "sfavorevoli" per gli algoritmi asimmetrici, come si può vedere dalla seguente tabella:

Simmetrica	Asimmetrica
56	384
64	512
80	768
112	1792
128	2304

Nel corso degli anni le raccomandazioni sulla lunghezza della chiave sono mutate, dato che la maggior potenza di calcolo riesce più facilmente a violare i codici criptati: la seguente tabella ne riporta le indicazioni a seconda degli utilizzatori:

Anno	Privato	Azienda	Governo
1995	768	1280	1536
2000	1024	1280	1536
2005	1280	1536	2048
2010	1280	1536	2048
2015	1536	2048	2048

L'idea che sembra essere la migliore è quella di prendere in blocco il messaggio e di crittografarlo in una sola volta: questa strada però non sempre è percorribile in quanto con chiavi lunghe il sistema diventerebbe troppo lento, anche con file di dimensioni modeste (qualche Kbyte).

La soluzione è quella di cercare di ottenere dal messaggio originale una sequenza di numeri (chiamata impronta o fingerprint o digest) più corta del messaggio stesso che sia unica, cioè che non consenta la generazione di altre sequenze identiche che possano essere interpretate come un messaggio diverso da quello che si vuole spedire.

A tale scopo vengono in aiuto le funzioni di hash, utilizzate nei sistemi MD4 e MD5 descritti in seguito.

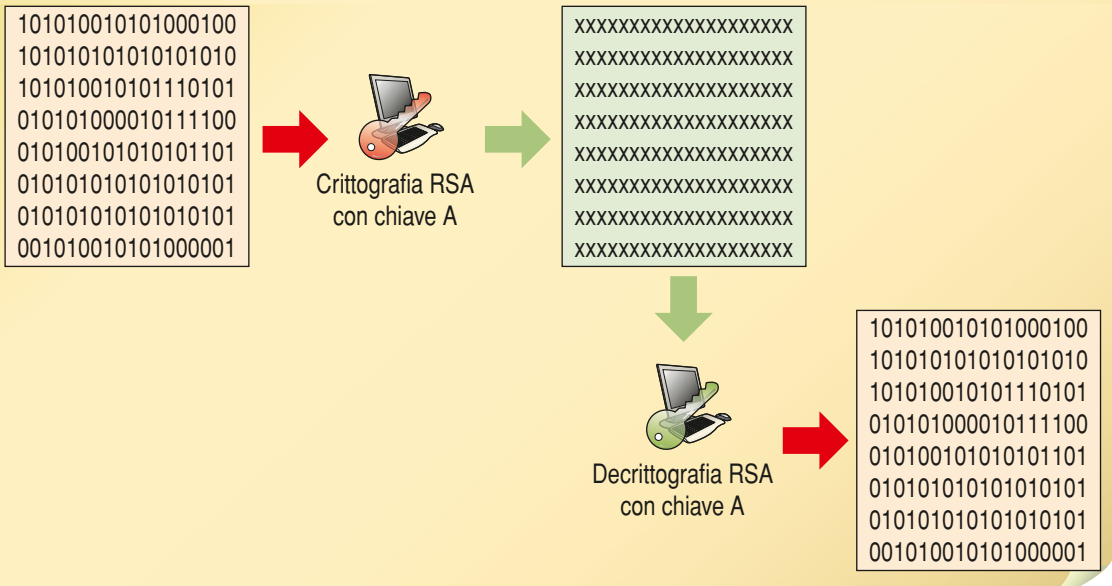
RSA

L'algoritmo RSA è stato descritto nel 1977 da Ronald Rivest, Adi Shamir e Leonard Adleman al MIT e fu brevettato nel 1983 negli Stati Uniti dal MIT (brevetto 4.405.829 scaduto nel settembre 2000). Abbiamo detto che il cuore della crittografia asimmetrica è una funzione facile da computare ma difficile da invertire, a meno di non conoscere un particolare dato (la chiave): l'algoritmo RSA "lavora" sfruttando i numeri primi e come chiave utilizza un numero n ottenuto proprio dal prodotto di due numeri primi p e q, cioè $n = p \cdot q$.

Per decrittare un messaggio cifrato con RSA è necessario decomporre la chiave n nei due numeri primi p e q: questo è computazionalmente impegnativo da ottenere, basti pensare che nel 2005 un gruppo di ricerca riuscì a scomporre un numero di 640 bit in due numeri primi da 320 bit impiegando per *cinque mesi* un cluster Opteron con 80 processori da 2,2 GHz.

Un attuale utilizzo è quello di sfruttare RSA per codificare un unico messaggio contenente una chiave segreta, tale chiave verrà poi utilizzata per scambiarsi messaggi tramite un algoritmo a chiave segreta (ad esempio AES).

Oggi RSA è uno degli algoritmi più usati per la cifratura di firme digitali, come descritto nella prossima lezione.



Descrizione dell'algoritmo

Il funzionamento dell'algoritmo RSA è il seguente:

1. A deve spedire un messaggio segreto a B;
2. B sceglie due numeri primi molto grandi e li moltiplica tra loro (generazione delle chiavi);
3. B invia ad A "in chiaro" il numero che ha ottenuto;
4. A usa questo numero per crittografare il messaggio;
5. A manda il messaggio a B, che chiunque può vedere ma non leggere;
6. B riceve il messaggio e utilizzando i due fattori primi, che solo lui conosce, decifra il messaggio.

Possiamo scomporlo in due componenti principali:

- la generazione delle chiavi;
- l'algoritmo crittografico vero e proprio.

Generazione delle chiavi

Il primo passo dell'algoritmo di generazione delle chiavi è quello di scegliere due numeri primi p e q e di calcolare il loro prodotto $n = p \cdot q$.

Quindi viene scelto un numero e, coprimo e più piccolo di $(p - 1)(q - 1)$ (chiamato esponente pubblico).

> Un numero a è coprimo di b se il massimo comune divisore tra a e b è 1.
> Ad esempio 5 e 13 sono coprimi, mentre 6 e 14 no, dato che hanno in comune il divisore 2.
>
> Se un numero a è primo, allora è coprimo di qualsiasi numero che non sia diviso da a.
> Ad esempio 11 è coprimo di tutti i numeri che non sono multipli di 11.

L'algoritmo di Euclide per il calcolo del MCD letto "al contrario" consente di esprimere il numero MCD(a,b) come combinazione lineare di a e b: permette di trovare due numeri interi r e s tali che

$$ra + sb = \text{MCD}(a,b)$$

Questa relazione, con semplici passaggi, ci permette di ottenere la seguente espressione che è alla base dell'algoritmo RSA:

$$d \cdot e = 1 \bmod m$$

e lo verifichiamo mediante il seguente esempio numerico.

ESEMPIO

Calcoliamo MCD(1789,1234) utilizzando l'algoritmo di Euclide (risulta MCD(1789, 1234) = 1) evidenziando i diversi quozienti ottenuti durante i vari passaggi.

x_i	1789	1234	555	124	59	6	5	1	0
q_i		1	2	4	2	9	1	5	

A partire dal MCD possiamo esprimere ciascun x_j come combinazione lineare di x_{i-2} e x_{i-1} (in grassetto i coefficienti della combinazione lineare):

$1 = 6 - (\mathbf{1} \cdot 5)$
$5 = 59 - (\mathbf{9} \cdot 6)$
$6 = 124 - (\mathbf{2} \cdot 59)$
$59 = 555 - (\mathbf{4} \cdot 124)$
$124 = 1234 - (\mathbf{2} \cdot 555)$
$555 = 1789 - (\mathbf{1} \cdot 1234)$

Ora, sostituendo nella prima uguaglianza il risultato della seconda, della terza, e così via, otteniamo:
$1 = 6 - (\mathbf{1} \cdot 5)$
$= 6 - \mathbf{1} \cdot (59 - \mathbf{9} \cdot 6) = -(\mathbf{1} \cdot 59) + (\mathbf{10} \cdot 6)$
$= -\mathbf{1} \cdot 59 + \mathbf{10} \cdot (124 - \mathbf{2} \cdot 59) = (\mathbf{10} \cdot 124) - (\mathbf{21} \cdot 59)$
$= \mathbf{10} \cdot (124 - \mathbf{21} \cdot (555 - 4 \cdot 124) = (-\mathbf{21} \cdot 555) + (\mathbf{94} \cdot 124)$
$= -21 \cdot 555 + 94 \cdot (1234 - \mathbf{2} \cdot 555) = (94 \cdot 1234) - (209 \cdot 555)$
$= \mathbf{94} \cdot 1234 - \mathbf{209} \cdot (1789 - 1 \cdot 1234) = (-\mathbf{209} \cdot 1789) + (\mathbf{303} \cdot 1234)$

Dunque: $-\mathbf{209} \cdot 1789 + \mathbf{303} \cdot 1234 = 1$
cioè: $\mathbf{303} \cdot 1234 = 1 - \mathbf{209} \cdot 1789$
e nella sua forma più generale: $\mathbf{303} \cdot 1234 = 1 + k(1789)$

che può essere scritta utilizzando l'operatore **mod** nella seguente espressione:

$303 \cdot 1234 = 1$ **mod** 1789

A partire da $n = p\ q$ e dalla relazione ottenuta dall'algoritmo di Euclide l'algoritmo RSA procede calcolando un numero d (chiamato *esponente privato*) tale che:

$$d \cdot e = 1 \bmod (p - 1)(q - 1)$$

Da questa espressione si ottiene:
- la chiave pubblica composta dalla coppia (e, n);
- la chiave privata composta dalla coppia (d, n).

I numeri p e q tali che $n = p\ q$ e che generano le coppie (e, n) e (d, n) sono conosciuti come numeri RSA.

ESEMPIO

Prendiamo ad esempio come numeri RSA $p = 3$, $q = 11$.

Calcoliamo

$$n = p \cdot q = 33 \ \text{ e } \ (p - 1)(q - 1) = 2 \cdot 10 = 20$$

Come numero coprimo minore di 20 scegliamo $e = 7$ e da questo individuiamo d tale che:

$$d \cdot e = 1 \bmod (p - 1)(q - 1)$$

Per calcolare d si può utilizzare quello che è chiamato metodo di Euclide esteso oppure andare per tentativi sostituendo un numero intero k nella seguente relazione, ottenuta dalla formula precedente, partendo da 1 e facendolo crescere fino a che si ottiene un numero intero:

Nel nostro caso viene subito soddisfatta per $k = 1$:

$$d = \frac{(k \cdot 20) + 1}{7} = \frac{(1 \cdot 20) + 1}{7} = \frac{21}{7} = 3$$

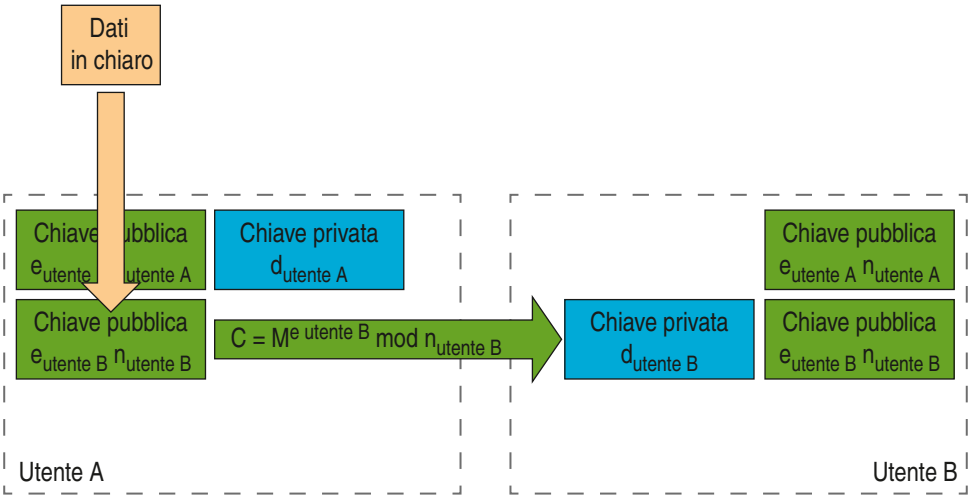
- la chiave pubblica è (7,33);
- la chiave privata è (3,33).

Algoritmo crittografico

A Cifratura del messaggio da parte del mittente

Il messaggio m che deve essere trasmesso viene innanzi tutto espresso in forma di numero e deve essere minore di n: questo può anche essere ottenuto suddividendolo in blocchi.

Il crittogramma c viene codificato calcolando come $c = m^e \bmod n$ (c risulta minore di n).



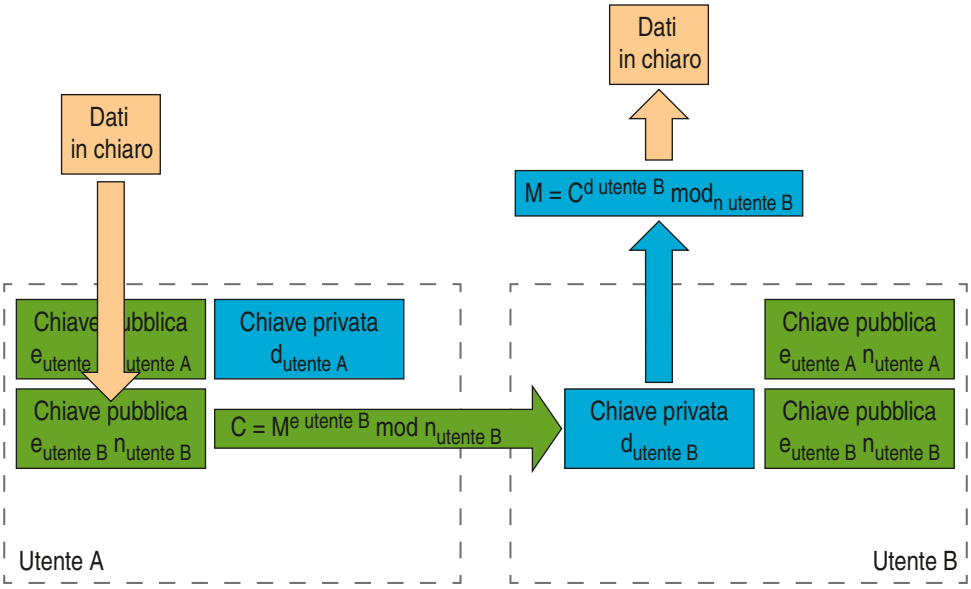
ESEMPIO

Volendo trasmettere il messaggio m = 9 con le chiavi precedenti, pubblica (7,33) e privata (3, 33), otteniamo:

$$c = m_{cifrato} = 9^7 = 4.782.969 \equiv 15(\mathrm{mod}33)$$

B Decifrazione del messaggio da parte del destinatario

Il messaggio m che giunge al destinatario viene decodificato calcolando $c^d \bmod n$



ESEMPIO

Utilizziamo come chiave privata (33, 7), otteniamo:

$$m_{chiaro} = 15^3 = 3365 \equiv 9(\text{mod}33)$$

A e B hanno impiegato pochi secondi a cifrare e decifrare, ma chiunque avesse intercettato le loro comunicazioni impiegherebbe milioni di anni per scoprire i due fattori primi con cui è cifrato il messaggio.

Lunghezza chiave	Tempo richiesto	Tempo richiesto
(bit)	a 1 decr/ms	a 10^6 decr/ms
56	2^{55} ms = 1142 anni	10 ore
128	2^{127} ms ~ 10^{24} anni	~ 10^{18} anni
168	2^{167} ms ~ 10^{36} anni	~ 10^{30} anni

La forza (o la debolezza) dell'algoritmo sta proprio qui, dato che si basa sull'assunzione mai dimostrata (nota come assunzione RSA, o RSA assumption) che il problema di calcolare un numero composto di cui non si conoscono i fattori sia computazionalmente non trattabile.

I metodi crittografici a chiave pubblica/privata come RSA possono inoltre essere impiegati per firmare digitalmente un messaggio garantendo con validità legale:

- l'autenticità della firma;
- la NON falsificabilità della firma;
- la NON riutilizzabilità della firma;
- la NON alterabilità del messaggio firmato;
- la NON ripudiabilità della firma.

In realtà questo sistema non è così semplice come ora descritto in quanto per trasmettere grandi quantità di dati occorre tanto tempo: verrà quindi utilizzato in un altro modo, ad esempio A e B si scambieranno con questo sistema una chiave segreta (che non occupa molto spazio), che poi useranno per comunicare tra loro usando un sistema a crittografia simmetrica, più semplice, sicuro e veloce (crittografia ibrida).

Crittografia ibrida

L'introduzione dei metodi a chiave pubblica come RSA ha risolto brillantemente il grande problema dello scambio della chiave: rimane comunque aperto il problema di dover gestire le chiavi pubbliche e quindi è necessario un sistema di PKI (Public Key Infrastructure) che si occupi della gestione e dello scambio delle chiavi.

Quindi le chiavi e i rispettivi proprietari sono associati in registri gestiti da un PKI, che può essere considerato come un "elenco telefonico" delle chiavi pubbliche.

Ma anche se la crittografia asimmetrica è stata una brillante intuizione le funzioni matematiche che generano il codice cifrato e quelle inverse per decifrarlo sono troppo lente per essere utilizzate nella cifratura di interi documenti, anche non di modeste dimensioni.

Sono nati sistemi di crittografia misti (o ibridi) che uniscono le due tecniche allo scopo di unirne i vantaggi.

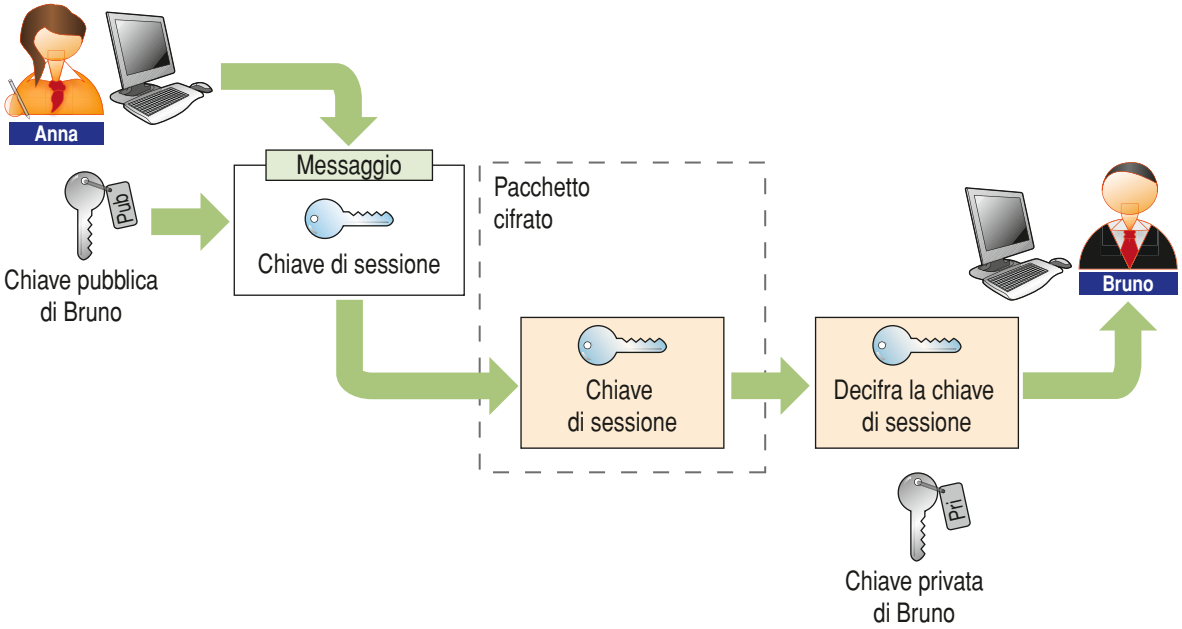
Crittografia simmetrica	Crittografia asimmetrica
Pro: molto veloce	Pro: non serve un canale sicuro per lo scambio delle chiavi
Contro: problema dello scambio delle chiavi	Pro: molto lenta, a causa dei calcoli complessi da effettuare

In un sistema ibrido utilizziamo la chiave pubblica soltanto per comunicare la chiave segreta (che in questi casi viene chiamata chiave di sessione) che poi verrà usata per una normale comunicazione basata su cifrati a chiave segreta.

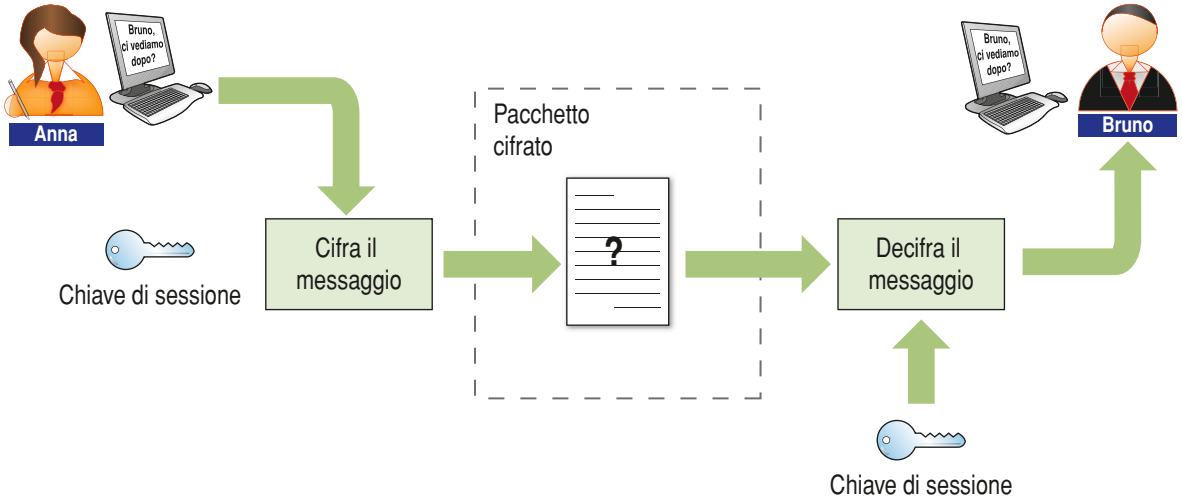
Così facendo non ci sono problemi di sicurezza in quanto la chiave che viene trasferita è di modeste dimensioni, inoltre è trasmessa una sola volta e, quando è stata ricevuta, può innescare un sistema di cifratura simmetrico tra i due interlocutori.

Vediamo nel dettaglio il funzionamento dove A e B devono comunicare in modo sicuro e veloce:

1. A predispone una chiave che verrà successivamente utilizzata per la cifratura simmetrica (chiave di sessione);
2. A utilizza la chiave pubblica di B per cifrare la chiave di sessione;
3. B decifra la chiave di sessione con la propria chiave segreta.



Ora A e B possono comunicare utilizzando la chiave di sessione per cifrare e decrittare i messaggi come in un sistema simmetrico.



Verifichiamo le competenze

1. Esercizi

1 Calcola la chiave pubblica (e,n) e privata (d,n) dati p = 7, q = 13, e = 11.

2 Calcola la chiave pubblica (e,n) e privata (d,n) dati p = 7, q = 17, e = 5.

3 Calcola la chiave pubblica (e,n) e privata (d,n) dati p = 61, q = 53, e = 17.

4 Calcola la chiave pubblica (e,n) e privata (d,n) dati p = 47, q = 71, e = 79.

5 Date le seguenti chiavi:
a) chiave pubblica: (7,33)
b) chiave privata: (3,33)
e volendo trasmettere il messaggio m = 15, cifra e decifra m utilizzando RSA.

6 Date le seguenti chiavi:
a) chiave pubblica: (5,65)
b) chiave privata: (29,65)
e volendo trasmettere il messaggio m = 7, cifra e decifra m utilizzando RSA.

7 Date le seguenti chiavi:
a) chiave pubblica: (17,3233)
b) chiave privata: (2753,3233)
e volendo trasmettere il messaggio m = 123, cifra e decifra m utilizzando RSA.

8 Date le seguenti chiavi:
a) chiave pubblica: 79,3337)
b) chiave privata: (1019,3337)
e volendo trasmettere il messaggio m = 688, cifra e decifra m utilizzando RSA.

9 Scrivi in un linguaggio a tua scelta l'algoritmo che sulla base dell'espressione:
$d \cdot e = 1 \bmod m$
conoscendo e e m ci permette di calcolare il valore di d (esponente privato), come nell'esempio descritto nel testo (come ad esempio 3031234 = 1 mod 1789).

Suggerimento
Per prima cosa si individua la legge di formazione dei coefficienti: si parte dalla coppia [0,1] e se [r,s] sono i coefficienti della combinazione lineare di 1 in funzione di xi−1 e xi allora [s, r − sqi] sono i coefficienti della combinazione lineare di 1 in funzione di xi e xi+1.

LEZIONE 3

Certificati e firma digitale

In questa lezione impareremo...

- la firma digitale e l'algoritmo MD5
- i certificati digitali

I sistemi di autenticazione

Crittare un messaggio completo può essere troppo dispendioso e lento; spesso non serve la segretezza ma basta l'autenticazione e la certezza che il messaggio non venga modificato.

In questi casi è sufficiente che il messaggio venga "imbustato" all'interno di un "contenitore digitale" che prende il nome di firma digitale che, oltre che a permettere di riconoscere se il documento stesso è stato modificato o meno dopo l'apposizione della firma, è soprattutto in grado di attestare la validità, la veridicità e la paternità di un documento elettronico e quindi, grazie a essa, è possibile risalire con certezza all'identità del firmatario.

La firma digitale è stata introdotta nella normativa europea dalla Direttiva 1999/93/CE ed è l'equivalente informatico di una tradizionale firma apposta su carta.

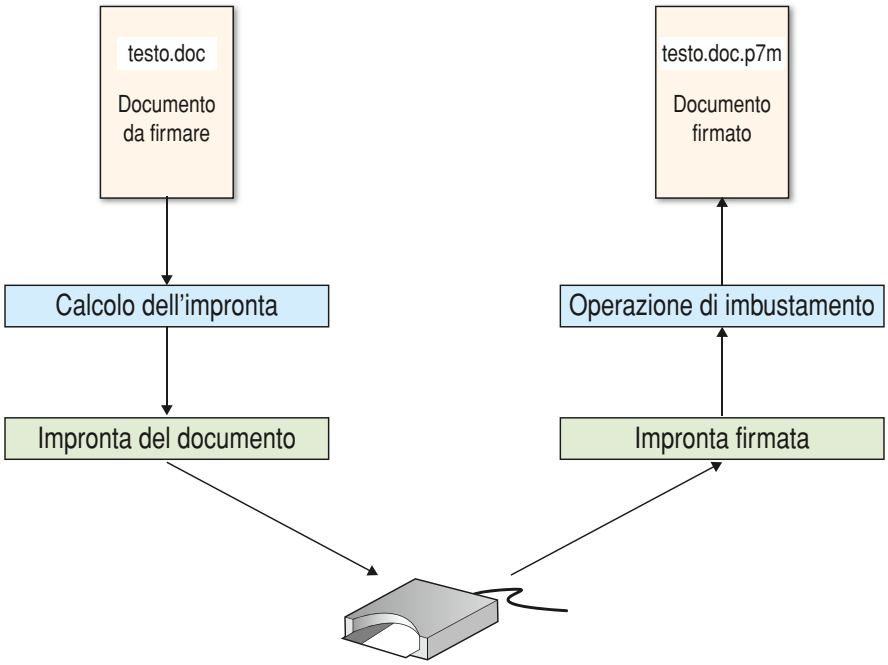
La firma digitale si basa su un sistema di codifica crittografica a chiavi asimmetriche che consente:
- la sottoscrizione di un documento informatico;
- la verifica, da parte dei destinatari, dell'identità del soggetto sottoscrittore;
- la certezza che l'informazione contenuta nel documento non sia stata alterata.

Operativamente l'utente possiede un dispositivo di firma sicuro (smart card o token USB o Business Key) rilasciato da appositi enti certificatori, i quali accertano l'identità del richiedente prima di consegnargli la carta: oltre al dispositivo l'utente viene dotato di codice segreto (PIN – Personal Identification Number) personale da utilizzarsi contemporaneamente alla smart card.

La Carta Nazionale dei Servizi (CNS) ideata per accedere ai servizi online della Pubblica Amministrazione su tutto il territorio nazionale, oltre che alla funzione di tessera sanitaria del SSN offre anche la possibilità di firma digitale oltre a un insieme di ulteriori servizi resi disponibili dalle diverse amministrazioni tra cui i pagamenti on line, il codice fiscale ecc.
http://www.progettocns.it/index.aspx

In figura sono riportate alcune tessere del SSN con le personalizzazioni regionali.

Durante l'apposizione della firma il file viene "incapsulato" in una busta crittografica e il risultato è un nuovo file, con estensione .p7m: la firma digitale in formato **p7m** consente di firmare qualunque tipo di file (rtf, doc, tiff, xls, pdf ecc.).



Il formato p7m, noto come formato pkcs#7, è quello previsto dalla normativa vigente sull'interoperabilità della firma digitale ed è quello che le Pubbliche Amministrazioni sono obbligate ad accettare. È il formato disponibile fin dagli albori, cioè il primo formato in uso fin dall'anno 1999, al quale si aggiunsero sette anni più tardi i formati di firma PDF e XML.

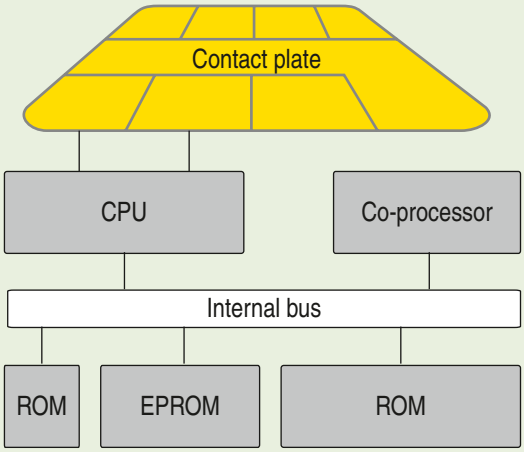
Gli enti di certificazione forniscono appositi programmi o servizi online per verificare l'identità del firmatario e la validità della firma apposta nel file p7m, permettendo di "aprire" il contenuto della "capsula p7m" e di leggere i dati che contiene.

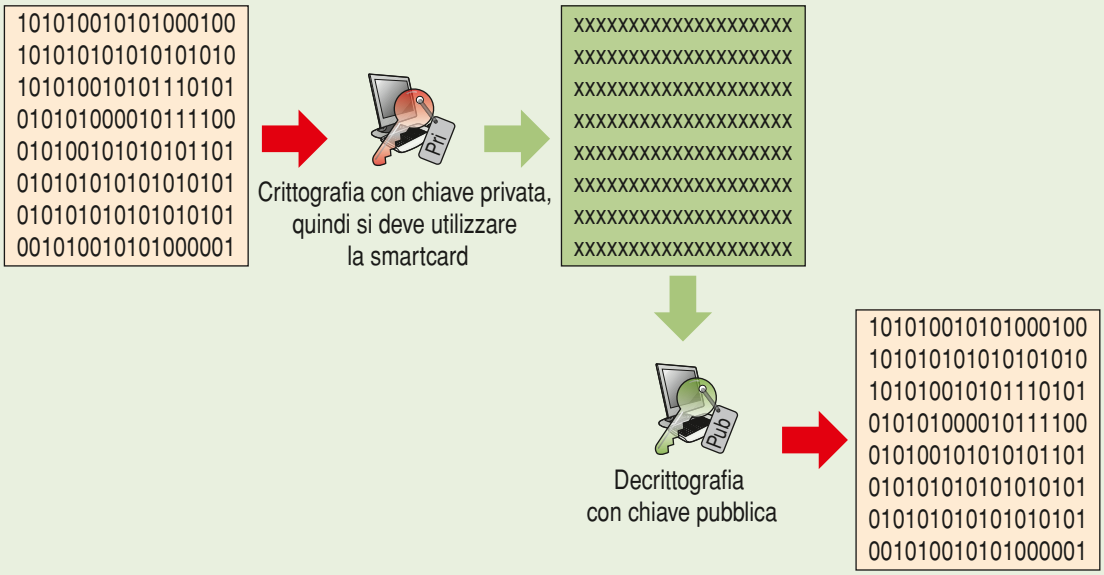
Zoom su...

SMART CARD

Per la legge italiana un dispositivo di firma idoneo è "*un apparato elettronico programmabile solo all'origine, facente parte del sistema di validazione, in grado almeno di conservare in modo protetto le chiavi private e generare al suo interno firme digitali. Il dispositivo di firma è il supporto candidato alla conservazione della chiave privata e deve dunque essere non riproducibile e, in parte, non modificabile.*
La chiave deve inoltre essere protetta da una procedura di identificazione del titolare (tipicamente l'inserimento di un PIN) e deve essere fatta in modo da non lasciare alcuna traccia della chiave privata sul sistema di validazione."

La smart card è il supporto più diffuso che risponde a tutti questi requisiti: è una tessera plastificata, con dimensioni di una carta di credito, su cui è integrato un microchip programmabile, con una ROM che contiene il sistema operativo e i programmi "fissi", una PROM che contiene il numero seriale della smartcard, una ROM che contiene i dati del proprietario e i meccanismi di protezione che ne evitano la clonazione.
Nella crittografia RSA la chiave pubblica e quella privata hanno una lunghezza minima di 1024 bit e vengono generate all'interno del dispositivo di firma (smartcard): la chiave privata non uscirà mai dal dispositivo mentre quella pubblica verrà resa nota e distribuita.



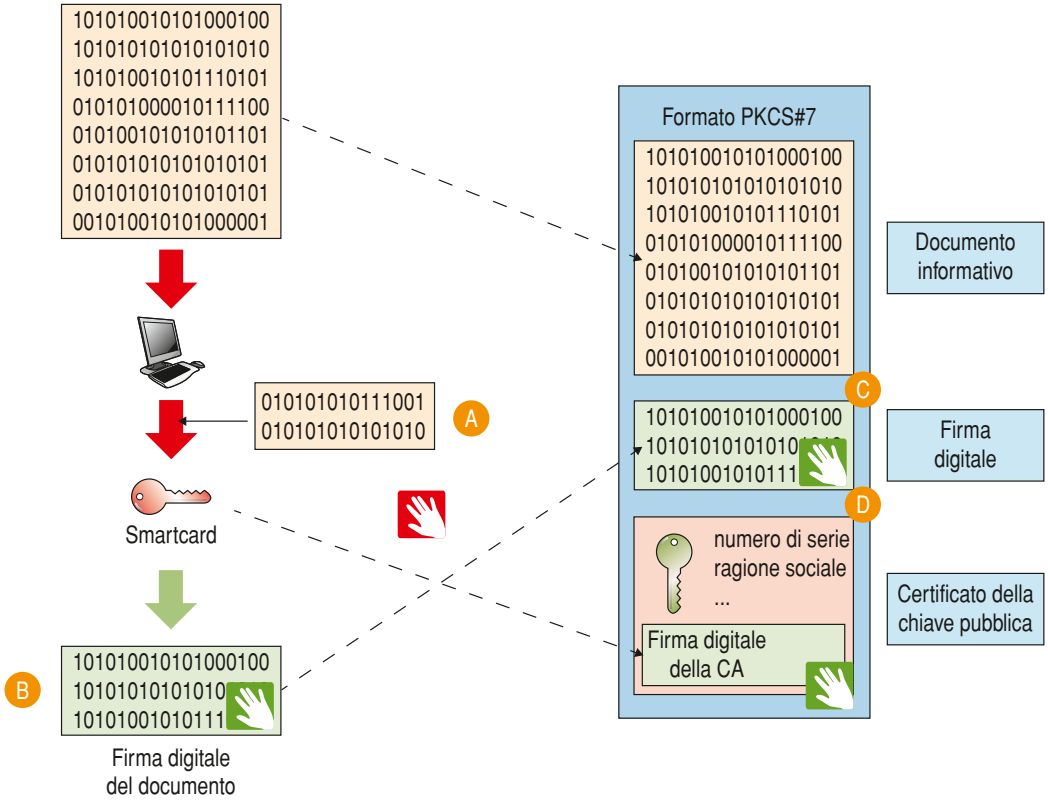


Firme digitali

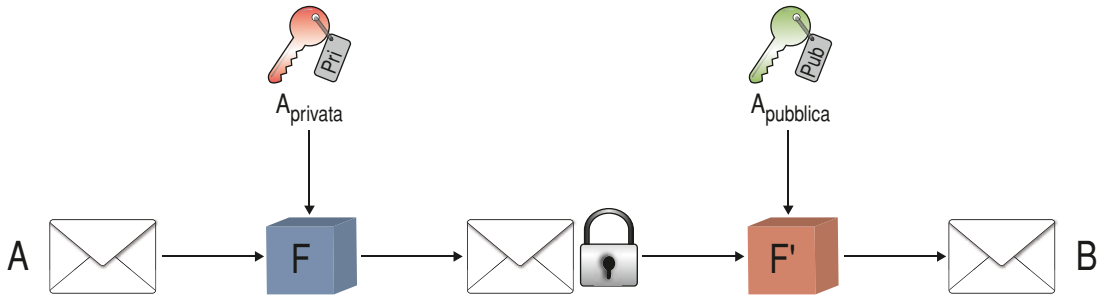
Tra le motivazioni per cui è nata la firma digitale è doveroso ricordare la lentezza dei sistemi di crittografia a chiave pubblica, incluso RSA: per rendere più efficiente il meccanismo si utilizza una funzione di hash attraverso la quale si calcola una stringa identificativa del messaggio, detta fingerprint (impronta digitale) o message digest composta da un numero limitato di caratteri.
Il calcolo della funzione di hash viene fatto in modo veloce così che risulta significativamente vantaggioso creare il fingerprint del messaggio e criptare quello con la propria piuttosto che criptare tutto il messaggio: in questo modo si autentica l'intero messaggio limitando l'uso dell'algoritmo di crittografia a chiave pubblica al solo fingerprint.

Quando A vuole mandare a B un messaggio autenticato e integro, calcola il fingerprint, lo cripta con la sua chiave privata e lo "aggancia" in fondo al messaggio in chiaro: la procedura è descritta di seguito:

- **A** da documento informatico si estrae l'impronta in chiaro (fingerprint);
- **B** l'impronta in chiaro viene cifrata, ad esempio con la smart card;
- **C** l'impronta crittografata viene "accodata " al messaggio in chiaro;
- **D** al messaggio viene anche accodato il *certificato del firmatario* (descritto in seguito).

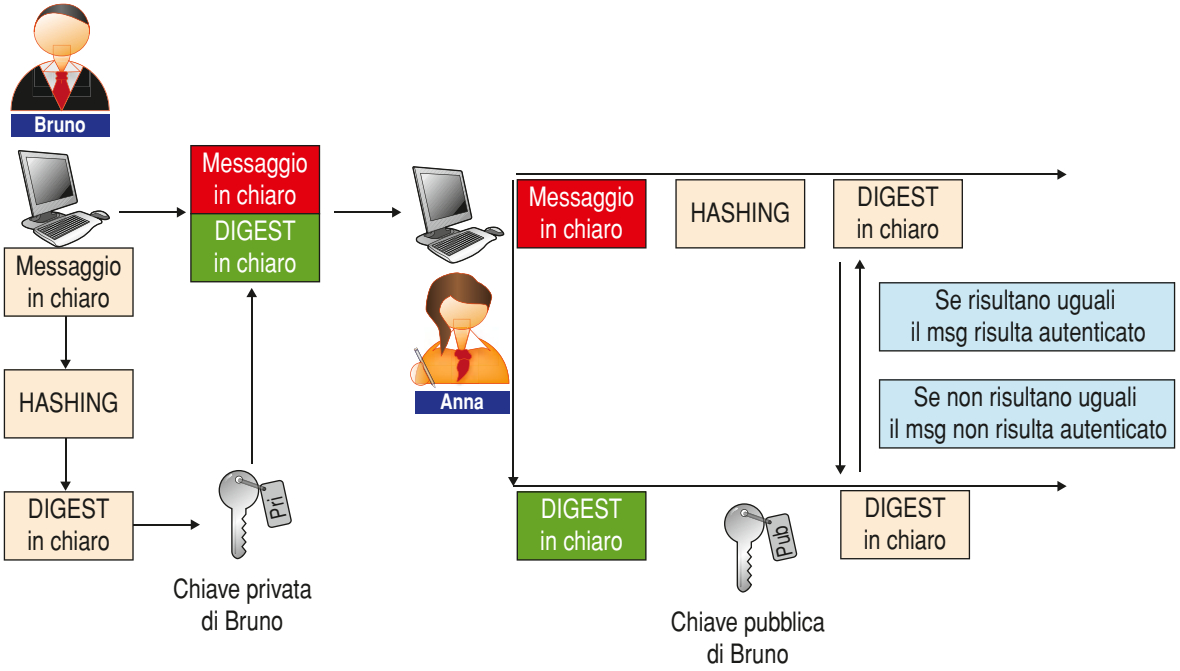


Il destinatario **B** per decriptare la firma deve utilizzare la chiave pubblica di **A** e solo questa è in grado di riconoscere il mittente, che quindi viene identificato come certo.



Con questo sistema è possibile anche verificarne l'integrità in quanto se il fingerprint ricalcolato sul messaggio ricevuto non corrisponde a quello inviato questo non risulta autenticato: in questo caso sicuramente il messaggio è stato alterato.

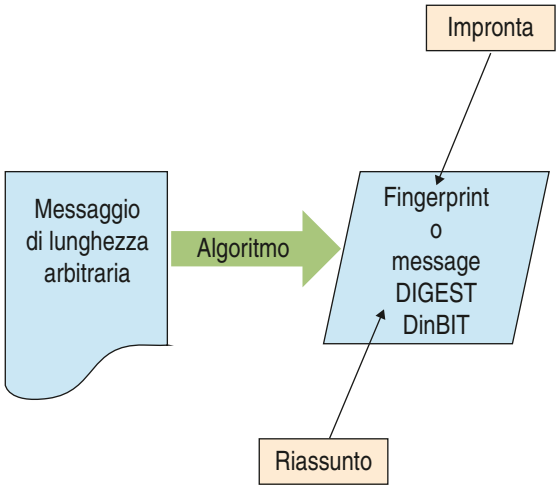
Lo schema di funzionamento può essere rappresentato in un figura:



Le funzioni Hash più note sono MD5 e SHA: MD5 è uno standard per Internet, è più insicuro ma veloce mentre SHA è uno standard governativo USA, molto più sicuro ma lento.

L'algoritmo MD5

L'algoritmo di sintesi più usato è MD5 (Message Digest 5), realizzato da Ronald Rivest nel 1991 e standardizzato con la RFC 1321, lo stesso Rivest che nel 1983 con Shamir e Leonard Adleman nel 1983 aveva brevettato RSA; è l'evoluzione dei precedenti MD2 e soprattutto MD4, del quale ha mantenuto la struttura ma ne ha migliorato la sicurezza.
La stringa risultante dall'operazione di hashing con MD5 è una stringa fissa di 128 bit, ossia 32 caratteri, chiamata MD5 Checksum o MD5 Hash, a partire da un messaggio di lunghezza qualsiasi. L'elaborazione è piuttosto complessa e prevede quattro fasi:



1. aggiunta bit di riempimento: ogni messaggio viene completato con una sequenza di 0 preceduti da un 1 (padding) fino a raggiungere un multiplo di 512;
2. aggiunta della lunghezza: gli ultimi 64 aggiunti contengono la una rappresentazione a 64-bit della lunghezza del messaggio originale;
3. inizializzazione del buffer MD (initial variable/chaining variable): viene predisposto un buffer di quattro word a 32-bit (128 bit) con dei particolari valori di inizializzazione;
4. elaborazione del messaggio (compression function): vengono definite quattro funzioni ausiliarie che ricevono in ingresso tre words da 32-bit e producono in uscita una sola word a 32-bit: successivamente ogni blocco di 16-word viene elaborato da un algoritmo particolarmente complesso che mescola completamente ogni blocco di 512 bit con il buffer di 128 bit, attraverso un procedimento in 4 passi.

Al termine il buffer contiene la sintesi del messaggio, cioè è generato il message digest.

Gli algoritmi SHA

Gli algoritmi SHA (acronimo di Secure Hash Algorithm) sono stati sviluppati dalla National Security Agency (NSA) e pubblicati dal National Institute of Standards and Technology. Gli algoritmi nascono come modifiche del MD4 e sono suddivisi in quattro categorie:

- SHA-0 : obsoleto
- SHA-1 : violato
- SHA-2 : in uso
- SHA-3 : annunciato nel 2012

L'algoritmo SHA-0 venne pubblicato nel documento FIPS PUB 180 nel 1993, e fu ritirato poco dopo la pubblicazione per essere sostituito dall'algoritmo SHA-1: entrambi producono un valore di hash di 160 bit. Fu violato nel 2005 da un gruppo di crittoanalisti cinesi.
Successivamente nacque la nuova versione dello standard, la SHA-2, che fu suddivisa in diverse famiglie a seconda della lunghezza in bit del codice hash.

> L'elaborazione eseguita dagli algoritmi SHA è sostanzialmente simile a quella del MD5, cioè è costituita da quattro fasi delle quali le prime due sono identiche mentre il passo 3 utilizza uno schema a 8 registri nel SHA-2 e nel passo 4 la sequenza di bit viene divisa in blocchi da 512 bit o 1024 bit a seconda dell'algoritmo: su ciascun blocco vengono effettuati 80 cicli di operazioni (compression function).

Nel novembre del 2007 venne indetto dal NIST un concorso aperto per la realizzazione di una nuova funzione SHA-3: il 2 ottobre 2012 fu annunciato come vincitore l'algoritmo Keccak, creato da un team di analisti italiani e belgi che gradualmente sostituirà la famiglia SHA-2, nonostante ancor oggi non sia stato violato.

I certificati digitali

Nei sistemi sino a ora descritti abbiamo trascurato un problema: abbiamo affermato che per verificare il mittente (Anna) il ricevente (Bruno) utilizza la sua chiave pubblica con la quale può "aprire" e autenticare il messaggio che gli è pervenuto. Ma come fa a essere certo che la chiave gli sia pervenuta effettivamente da Anna e non da un intruso "mascheratosi" da Anna?

La soluzione di questo problema, che consiste nel certificare l'identità del mittente, viene fatta attivando una particolare procedura per la consegna della chiave pubblica da Anna a Bruno: la chiave viene racchiusa all'interno di un certificato digitale che oltre a essa contiene le informazioni sul mittente.

Questo certificato deve essere a sua volta validato da un ente certificatore (CA Certification Authority) che garantisce l'identità del proprietario del certificato firmandone le chiavi pubblica e privata con la propria chiave privata: in questo modo ne rende impossibile per chiunque la manomissione.

Un malintenzionato dovrebbe effettuare le seguenti operazioni per sostituirsi ad Anna:

1. violare la cifratura del CA che protegge le due chiavi;
2. sostituire le chiavi originali con delle chiavi fasulle;
3. ricodificare il tutto con la chiave privata della Certification Authority.

Possiamo quindi essere abbastanza tranquilli perché sembra impossibile effettuare tutte queste operazioni anche per un abile hacker!

Quindi il Certificato Digitale è un documento informatico contenuto nella smartcard del titolare e firmato digitalmente dal certificatore.
I dati contenuti nel certificato sono quindi seguenti:

- dati del proprietario, tra cui il nome, cognome e data di nascita del titolare e la chiave pubblica;
- dati del certificato, tra cui la data di scadenza e il numero di serie del certificato;
- dati della Certification Authority, ovvero la ragione sociale del certificatore, il codice identificativo del titolare presso il certificatore e la firma digitale.

Una coppia di chiavi a 1024 bit può avere validità massima di 2 anni.

Le pratiche relative alla identificazione dell'utente prima della emissione del certificato vengono fatte dalla Registration Authority che, in base alla tipologia del soggetto che richiede il certificato, svolge le necessarie indagini e attiva le relative procedure per l'identificazione certa del richiedente: la Certification Authority si occupa invece più specificatamente del "ciclo di vita del certificato", gestendone la sua pubblicazione online e relativa manutenzione.

Registration Authority e Certification Authority, per la delicatezza del ruolo che svolgono, sono enti pubblici o privati **accreditati** selezionati che devono aver richiesto e ottenuto il riconoscimento del possesso dei requisiti più elevati in termini di qualità e di sicurezza.

Un certificato digitale può avere diversi formati, tra i quali i più diffusi sono:

- chiavi PGP/GPG;
- certificati X.509.

La differenza sostanziale tra un certificato PGP/GPG e uno di tipo X.509 è che è possibile creare il proprio certificato PGP/GPG in modo autonomo e in pochissimi istanti, mentre per X.509 è necessario rivolgersi a un ente addetto allo scopo.

L'insieme costituito da tutte le parti, utenti e Authority, nonché dalle tecnologie che queste utilizzano, dai servizi che offrono e dalle politiche di gestione che attuano, è detto PKI (Public Key Infrastructure).

Public Key Infrastructure PKI

La Public Key Infrastructure è l'infrastruttura tecnica e organizzativa preposta alla creazione, distribuzione e revoca dei certificati di chiave pubblica: è organizzata come una foresta di Certification Authority dove come radice, che prende il nome di CA root, è presente l'ente titolare della gestione del PKI.

Quindi gli enti certificatori che hanno lo status di root possono firmare i certificati di altri enti che possono essere sia utenti finali (le foglie) che altre aziende certificatrici (nodi intermedi): questi definiscono inoltre i protocolli, le politiche e i meccanismi tecnologici necessari per supportare lo scambio autenticato di chiavi pubbliche.

Una PKI può essere pubblica o privata: in questo caso i servizi offerti sia di autenticazione che di certificazione globale, possono essere non gratuiti, ma regolati da contratti e accordi commerciali.

I PKI gestiscono un repository dei certificati dove memorizzano e pubblicano i certificati e le liste di quelli revocati (CRL: Certificate Revocation List): vengono revocati i certificati per le chiavi pubbliche le cui corrispondenti chiavi private vengono compromesse, oppure per chiavi pubbliche le cui chiavi private sono andate perse oppure non più usate dai legittimi proprietari perché, ad esempio, licenziati o trasferiti oppure per semplice scadenza temporale della validità.

Richiedere un certificato digitale

Vediamo brevemente come si ottiene un certificato digitale: la procedura è abbastanza standard e le piccole differenze tra i diversi CA possono riguardare i dati da fornire o in merito alla procedura di generazione e comunicazione della coppia di chiavi asimmetriche.
Possiamo individuare quattro passi:

1. generazione della coppia di chiavi asimmetriche da utilizzare per cifrare le comunicazioni: le comunicazioni tra CA e richiedente devono essere protette e quindi viene generata una coppia di chiavi dal CA direttamente seguendo la procedura indicata sul suo sito;
2. il richiedente comunica informazioni circa la propria identità alla Certification Authority: ricevute le chiavi è ora possibile comunicare le informazioni riguardanti il richiedente quali il nome di dominio, l'indirizzo email, il nome e cognome del richiedente ecc.;
3. la Registration Authority inizia la verifica dei dati ricevuti: le operazioni di controllo dei dati pervenuti alla CA possono variare a seconda del soggetto e del tipo di certificato richiesto e in questa fase possono essere richiesti anche ulteriori dati, come ad esempio l'iscrizione alla Camera di Commercio o la partita IVA;
4. se i controlli vanno a buon fine, la Certification Athority genera il certificato e lo firma digitalmente con la propria chiave privata: viene cifrato per garantire che i dati in esso contenuti non vengano modificati;
5. il certificato firmato viene inviato al richiedente che provvederà a installarlo o a farlo installare sul proprio server.

Esistono numerosi programmi di utilità che consentono di criptare file, dischi o dati in generale, vediamone alcuni.

Gestione file

- FileDecoder: Crea file cifrati con password.
- FileVault: Crea file auto-estraenti e auto-decifranti (che quindi non necessitano di alcun software).
- Kleopatra: Unisce alla crittografia la gestione dei certificati, permette di criptare file e certificati.
- AxCrypt: Permette di cifrare, comprimere, decifrare, eliminare, visualizzare e modificare i file in modo facile e veloce.
- Kruptos: Permette di cifrare i file sia su PC che dispositivi mobili. E' in grado di generare file auto-decifranti.

Disco Fisso
- CryptoExpert: Crea dischi fissi virtuali cifrati.
- VeraCrypt: Crea dischi fissi cifrati.

Dati
- Data Scrambler: Trasforma i dati in un'immagine bitmap con algoritmo MD5.
- PixelCryptor: Software per cifrare dati attraverso immagini.

Riferimenti normativi

La legislazione italiana, con successivi interventi normativi, ha rivoluzionato il mondo burocratico-amministrativo, attribuendo alla firma digitale lo stesso valore della firma autografa, rendendo pienamente validi ai fini di legge i documenti informatici sottoscritti digitalmente.

Con l'entrata in vigore della L. 15/3/1997, n. 59 sulla semplificazione amministrativa (la c.d. Bassanini uno), gli atti e i documenti di provenienza pubblica e privata sono formalmente entrati nell'era digitale.
L'art. 15, comma 2, stabilisce infatti che "gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi a tutti gli effetti di legge".

Il Codice dell'Amministrazione Digitale, ha la finalità di assicurare che tutte le P.A. adottino strumenti per rendere sempre disponibili tutte le informazioni in modalità digitale: l'art. 21, comma 2, dispone che il documento informatico sottoscritto con firma digitale o con altro tipo di firma elettronica avanzata, "ha l'efficacia prevista dall'articolo 2702 del codice civile".

Il D.P.C.M. 13/1/2004, contenente le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici, regola gli aspetti tecnici e organizzativi di chi usufruisce e opera con i documenti informatici e la firma digitale.

La Deliberazione CNIPA 4/2005 del 17 febbraio 2005 (sostituita dalla successiva Deliberazione CNIPA 45/2009) descrive le regole e gli standard per l'interoperabilità dei Certificatori iscritti all'elenco pubblico presso il CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione).

DPCM del 30 marzo 2009 e la successiva Deliberazione CNIPA del 21 maggio 2009 n.45 contiene le regole tecniche in materia di generazione, apposizione e verifica della firma digitale e validazione temporale dei documenti informatici.
Grazie alla definizione di questi standard e a regole comuni i Certificatori italiani hanno ottenuto il riconoscimento della validità di documenti scambiati tra soggetti aventi firme certificate da differenti CA; inoltre le Pubbliche Amministrazioni, le imprese e i privati possono scambiarsi documenti elettronici con la stessa validità dei corrispondenti documenti cartacei.

Verifichiamo le conoscenze

1. Risposta multipla

1 La firma digitale si basa su un sistema di codifica a chiavi asimmetriche che consente:

a. la sottoscrizione di un documento informatico
b. la verifica, da parte dei destinatari, dell'identità del soggetto sottoscrittore
c. la verifica, da parte del mittente, dell'avvenuta consegna al destinatario
d. la certezza che l'informazione contenuta nel documento non sia stata alterata

2 Per la legge italiana un dispositivo di firma idoneo è (indicare l'affermazione errata):

a. un apparato elettronico programmabile solo all'origine
b. facente parte del sistema di validazione
c. in grado almeno di conservare in modo protetto le chiavi private
d. generare al suo interno firme digitali
e. una tessera plastificata, con dimensioni di una carta di credito

3 L'estensione di un file firmato digitalmente è:

a. p7m b. pm7 c. m7p d. mp7

4 Una impronta digitale di un messaggio gode di tre importanti proprietà:

a. è sempre facile calcolare il valore di hash di un messaggio
b. è generata da una chiave privata
c. è impossibile risalire al messaggio partendo da un dato valore di hash
d. è poco probabile che due messaggi diversi abbiano la stessa sintesi

5 L'acronimo PGP deriva da:

a. Privacy Good Pretty
b. Pretty Good Privacy
c. Privacy Global Pretty
d. Pretty Global Privacy

2. Ordinamento

1 Ordina le quattro fasi dell'algoritmo MD5:

a. ..... inizializzazione del buffer MD
b. ..... aggiunta della lunghezza
c. ..... aggiunta bit di riempimento
d. ..... elaborazione del messaggio

3. Vero o falso

1 La firma digitale è stata introdotta nella normativa europea dalla Direttiva 1999/93/CE. V F
2 Per la legge italiana la smart card è un dispositivo di firma idoneo. V F
3 Una funzione di hash è chiamata one way hash se non è reversibile. V F
4 L' impronta digitale o message digest è composta da un numero limitato di caratteri. V F
5 Il fingerprint viene criptato con la chiave privata e agganciato in fondo al messaggio in chiaro. V F
6 La smartcard è necessaria per decrittare un documento cifrato. V F
7 Nel MD5 ogni messaggio ha un padding per raggiungere un multiplo di 512. V F
8 Con l'MD5 occorrono circa 100 ore per trovare collisioni. V F
9 L'algoritmo SHA-0 fu violato nel 2005 da un gruppo di crittoanalisti cinesi. V F
10 SHA-2 si trova alla base di applicazioni per la sicurezza come PGP e SSL. V F
11 Una coppia di chiavi a 1024 bit può avere validità massima di 3 anni. V F
12 Tra i formati di certificato digitale più diffusi troviamo il X.609. V F

Esercitazioni di Laboratorio 1

L'ALGORITMO DI CIFRATURA RSA IN C++

RSA

◀ RSA ▶ è un algoritmo di cifratura a chiave pubblica che permette di cifrare un messaggio sfruttando alcune proprietà elementari dei numeri primi. Questo cifrario prende il nome dalle iniziali dei ricercatori del MIT che lo idearono nel 1978: Rivest, Shamir e Adleman. La loro idea fu quella di sfruttare la difficoltà nel fattorizzare un numero intero: infatti la chiave pubblica utilizzate è rappresentata da un numero N ottenuto moltiplicando due numeri primi (segreti) molto grandi.

◀ Il sistema di crittografia si basa sull'esistenza di due chiavi distinte, che vengono usate per cifrare e decifrare. Se la prima chiave viene usata per la cifratura, la seconda deve necessariamente essere utilizzata per la decifratura e viceversa. La questione fondamentale è che nonostante le due chiavi siano fra loro dipendenti, non sia possibile risalire dall'una all'altra, in modo che, se anche si è a conoscenza di una delle due chiavi, non si possa risalire all'altra, garantendo in questo modo l'integrità della crittografia. ▶

Per aumentare la sicurezza del metodo è consigliabile fare uso di chiavi binarie minimo di 2048 bit, le chiavi a 512 bit sono infatti craccabili in poche ore. Le chiavi a 1024 bit sono ancor oggi largamente diffuse e utilizzate in sistemi di sicurezza di una certa importanza, infatti mediante l'algoritmo GNFS (General Number Field Sieve) si riescono a ◀ fattorizzare ▶ numeri N dell'ordine di 2^{768}-10^{231}.

◀ Attraverso l'uso di un computer cluster molto potente, del costo di centinaia di migliaia di Euro, potrebbero essere ricavate chiavi a 768 bit (ordine di 2^{768}) all'incirca dopo 6 mesi di attacco. Pertanto chiavi a 1024 bit o superiori sono al momento fuori dalla portata di un attacco realistico. ▶

Algoritmo RSA

Vediamo il funzionamento dell'algoritmo RSA:

1. Si scelgono due numeri primi, p e q sufficientemente grandi. Ricordiamo a titolo di esempio che i numeri primi utilizzati per chiavi a 2048 bit utilizzano oltre 300 cifre decimali.
2. Si calcolano due prodotti:
   - il prodotto $n = p * q$, chiamato modulo n
   - il prodotto $f(n) = (p - 1) * (q - 1)$

Come possiamo notare il calcolo di n si ottiene in pochi centesimi di secondo, mentre invece la scomposizione di n, necessaria per un attacco con il quale ottenere p e q, richiede un tempo elevatissimo: questo fa di RSA un algoritmo assai robusto.

3. Si sceglie un numero e chiamato esponente pubblico, co-primo con f(n), inferiore rispetto a f(n). Ricordiamo che e e f(n) sono primi tra di loro, cioè l'MCD tra e e f(n) è 1.
4. Si calcola il numero d chiamato esponente privato tale che (e * d) % f(n) = 1.

Esistono due metodi, i generale, per attaccare l'algoritmo RSA:
- mediante un algoritmo che, dato un testo cifrato c e la chiave pubblica (N; e), restituisca il testo decifrato m senza tuttavia ottenere la chiave privata (N; d);
- mediante un algoritmo che ricavi la chiave privata (N; d) da quella pubblica (N; e).

ESEMPIO

Generazione chiave pubblica e privata

Vediamo adesso un esempio che mostra come generare le due chiavi, pubblica e privata:
1. Si scelgono 2 numeri primi (in questo caso molto piccoli per facilitare il calcolo): p = 11 e q = 31.
2. Calcoliamo n = p * q = 11 * 31 = 341.
3. Calcoliamo f(n) = (p – 1) * (q – 1) = 10 * 30 = 300.
4. Prendiamo e = 17, dato che e < 300 ed e è coprimo di 300.
5. Scegliamo d = 2753.
6. Chiave pubblica k = (n, e) = (341, 17);
   Chiave privata h = (n, d) = (341, 2753).

Per cifrare il testo in chiaro (chiamato m) utilizziamo la formula seguente che utilizza la chiave pubblica:

$$c = (m^e) \% n$$

Per decifrare il testo cifrato (c) e ottenere nuovamente m, cioè il testo decifrato, utilizziamo la chiave privata:

$$m = (c^d) \% n$$

Codifica del programma

Vediamo come decodificare in linguaggio C++ l'algoritmo di cifratura secondo il metodo RSA. Si tratta di un programma a titolo di esempio, non è pertanto ammissibile l'inserimento di p e q troppo grandi, che potrebbero causare l'overflow del tipo unsigned long: in generale devono essere minori di 3232.
Inoltre sia nella cifratura che nella decifratura del messaggio, abbiamo utilizzato la formula $(m \% n)^e$ al posto di $m^e \% n$.
Vediamo innanzi tutto la funzione che calcola l'MCD in modo ricorsivo, tramite la funzione MCD() che restituisce il massimo comun divisore tra i due parametri (a e b) passati:

```
unsigned long MCD(unsigned long a, unsigned long b)
{
  //Funzione ricorsiva che calcola MCD tra a e b
  unsigned long r = a % b;
  if (r == 0)
    return b;
  return MCD(b,r);
}
```

La funzione seguente (cifratura()) effettua la cifratura del messaggio m passato unitamente all'array k[] che contiene come nelle posizioni 0 e 1 i due valori della chiave pubblica:

```
unsigned long cifratura(unsigned long k[], unsigned long m)
{
  //funzione che cifra il messaggio m con la chiave pubblica k[]
  unsigned long s = 1;
  for (unsigned long i = 0; i < k[1]; i++)
  {
    s = (s * m) % k[0];
  }
  return s;
}
```

La funzione decifratura() invece effettua l'operazione opposta rispetto alla funzione precedente. Per fare questo riceve come parametro il messaggio cifrato (c) e la chiave privata h[], anche in questo caso rappresentata da un Array:

```
unsigned long decifratura(unsigned long h[], unsigned long c)
{
  //funzione che decifra il messaggio c con la chiave privata h[]
  unsigned long s = 1;
  for (unsigned long i = 0; i < h[1]; i++)
  {
    s = (s * c) % h[0];
  }
  return s;
}
```

Vediamo adesso la parte iniziale del programma, come possiamo notare sono inclusi i file iostream e cmath, quindi vengono indicati i prototipi delle funzioni. Le variabili di tipo unsigned long consentono di avere numeri interi positivi molto grandi, anche se non sufficienti per rendere l'algoritmo seriamente utilizzabile. Successivamente vengono letti i valori di p e q, ricordando che l'utente può inserire dei numeri primi inferiori a 3232. Quindi viene effettuato il calcolo di n e f(n).

```
#include <iostream>
#include <cmath>
using namespace std;
//Prototipi funzioni
unsigned long cifratura(unsigned long k[], unsigned long m);
unsigned long MCD(unsigned long a, unsigned long b);
unsigned long decifratura(unsigned long h[], unsigned long c);
//Main program
int main()
{
  unsigned long p;
  unsigned long q;
  //Inserimento numeri primi p e q
  cout << "Inserisci p: ";
  cin >> p;
  cout << "Inserisci q: ";
  cin >> q;
  //Calcolo del prodotto tra p e q = n
  unsigned long n = p * q;
  unsigned long f = (p - 1) * (q - 1);
  cout << "n    = p * q          : " << n << endl;
  cout << "f(n) = (p-1)*(q-1)    : " << f << endl;
```

Il codice successivo dopo aver fissato un valore predefinito per l'esponente pubblico e, verifica se il valore calcolato di f è compatibile (MCD tra e e f(n) è diverso da zero e e < f(n)). Quindi viene effettuato il controllo sull'esponente privato d. Infine viene cifrato e decifrato il messaggio attraverso la chiamata delle funzioni cifratura e decifratura:

```
  //e inserito nel programma a titolo di esempio
  unsigned long e = 17;
  //Se l'MCD tra e ed f(n) è 1 il programma prosegue altrimenti esce
  if (!(MCD(e, f) == 1 && e < f))
  {
    //Forza l'uscita dal programma
    return -1;
  }
  cout << "Esponente pubblico e     : " << e << endl;
  unsigned long d = 2753;
  //Se d (e*d)%f(n)=1 il programma prosegue altrimenti esce
  if (!((e * d) % f == 1))
  {
    //Forza l'uscita dal programma
    return -1;
  }
  cout << "Esponente privato d      : " << d << endl;
  //Array k[] chiave pubblica array h[] chiave privata
  unsigned long k[] = {n, e};
  unsigned long h[] = {n, d};
  cout << "Chiave pubblica          : k(" << k[0] << "," << k[1] << ")" << endl;
  cout << "Chiave privata           : h" << h[0] << "," << h[1] << ")" << endl;
  //1) Inserimento del numero da cifrare (max 3232)
  unsigned long m;
  cout << "Messaggio da cifrare     : m=";
  cin >> m;
  unsigned long c = cifratura(k, m);
  cout << "Cifratura di m           : c= " << c << endl;
  m = decifratura(h, c);
  cout << "Decifratura di c         : m= " << m << endl;
  system("PAUSE");
  return 0;
}
```

L'esecuzione del programma con p=11 e q=31 è la seguente:

```
Inserisci p: 11
Inserisci q: 31
n     = p * q              : 341
f(n)  = (p-1)*(q-1)        : 300
Esponente pubblico e       : 17
Esponente privato d        : 2753
Chiave pubblica            : k(341,17)
Chiave privata             : h341,2753)
Messaggio da cifrare       : m=15
Cifratura di m             : c= 302
Decifratura di c           : m= 15
Premere un tasto per continuare . . .
```

Prova adesso!

- Applicare la cifratura RSA

APRI IL FILE algoritmo_rsa.cpp

1. Prova a eseguire l'esempio con numeri primi che non possano essere contemplati dall'algoritmo e verifica che il programma non stampi i valori degli esponenti pubblico e privato. Annota i valori di almeno 5 coppie di numeri ed effettua un controllo incrociato facendo i calcoli mediante la calcolatrice.
2. Modifica il codice del programma effettuando il controllo sui numeri *p* e *q* inseriti. Se non sono primi il programma deve richiederli nuovamente.
3. Modifica il codice permettendo l'inserimento di una stringa come messaggio (*m*), convertendola poi nel relativo codice ASCII.

Esercitazioni di Laboratorio 2

UN ALGORITMO DI CIFRATURA CON PHP: MD5

Introduzione alla crittografia in PHP

Attualmente la crittografia è utilizzata in moltissimi campi dell'Information Technology. Per iniziare proponiamo alcuni di esempi di applicazione della crittografia: ad esempio le password sono memorizzate nelle tabelle dei database in forma crittografata, oppure esistono i cosiddetti Tunnel cifrati attraverso Internet che vengono resi possibili con i protocolli SSL, SSH, e altre tecnologie, oppure ancora le reti private virtuali (VPN). Un metodo di crittografia assai diffuso è Pretty Good Privacy (PGP) che consente di difendere i dati, come ad esempio file o informazioni di posta elettronica.
Lo sviluppatore PHP deve essere consapevole che le pratiche di sicurezza sono ormai diventate indispensabili, dato il diffondersi di attacchi alle informazioni e di diffusione delle stesse tecnologie di difesa che le rendono via via sempre più vulnerabili. I metodi che rendono sicure le pagine possono essere i più banali, come ad esempio un campo password non mostrato in chiaro in una pagina di login, fino ai più sofisticati, come ad esempio l'utilizzo di metodi crittografici quali: DES, MD5, SHA1, Blowfish.

MD5 in PHP

L'algoritmo di sintesi più usato è MD5 (Message Digest 5), realizzato da Ronald Rivest nel 1991, lo stesso Rivest che nel 1983 con Shamir e Leonard Adleman nel 1983 brevettò RSA, e standardizzato con la RFC 1321: è l'evoluzione dei precedenti MD2 e soprattutto MD4, del quale ha mantenuto la struttura ma ne ha migliorato la sicurezza.
La crittografia tramite algoritmo MD5 viene applicata in tutti i settori dell'informatica che lavorano con il supporto delle firme digitali o che comunque trattano dati sensibili.

> Un utilizzo dell'MD5 è anche quello che garantisce l'integrità dei dati, controllando quindi che uno scambio di dati sia avvenuto senza perdite attraverso il confronto della stringa prodotta dal file inviato con quella prodotta dal file ricevuto.

I motori di ricerca la utilizzano per verificare se un file è cambiato e quindi una pagina deve essere nuovamente indicizzata.

Il linguaggio PHP lo utilizza grazie a una funzione nativa ad esempio per l'autenticazione degli utenti, durante la registrazione di un utente su un portale Internet: la password scelta durante il processo verrà codificata tramite MD5 e la sua firma digitale verrà memorizzata nel database.

Per realizzare un semplice script che utilizza MD5 in php basta richiamare la funzione md5() che è una built-in del linguaggio come nel codice sotto riportato:

md5/cifra.php

```
1  <?php
2  // lettura variabile da criptare
3  $txt = $_GET['testo'];
4
5  // funzione di criptaggio
6  $txt_cifrato = md5($txt) ;
7
8  echo "<font color='#006600'><strong>Il testo cifrato &egrave;:</strong></font>
9  <br/>".$txt_cifrato."<br/><br/>";
10
11 ?>
12
```

Mandando in esecuzione la pagina HTML che richiama questo segmento di codice otteniamo: ◀

Il codice è scaricabile dalla sezione materiali del sito www.hoepliscuola.it dedicato a questo volume: per mandarla in esecuzione basta copiare i file in una cartella MD5 creata nella cartella htdocs di Xampp e digitare la url nel browser http://localhost/md5.

Prova adesso!

• Applicare l'algoritmo MD5

1. Crea un pagina PHP per la gestione dell'autenticazione dell'utente, richiedendo come userId un indirizzo di posta e una password di lunghezza almeno di 8 caratteri che siano composti da:
   - almeno un carattere minuscolo;
   - almeno un carattere maiuscolo;
   - almeno un numero;
   - almeno un carattere di controllo.
2. Codifica la password inserita con MD5 e memorizzala in un archivio: quindi in una seconda pagina segnala all'utente la conferma dell'autenticazione oppure la richiesta di inserimento nel database dei suoi dati nel caso che il suo nominativo non fosse presente.

Esercitazioni di Laboratorio 3

LA CRITTOGRAFIA IN PHP: FORM SICURO CON CRYPT()

Form non sicuro senza crittografia

In questa lezione affrontiamo le tematiche essenziali per lo sviluppo di applicazioni che rispondano ai canoni di sicurezza e privacy delle informazioni, utilizzando le funzioni residenti del linguaggio PHP. Vediamo adesso un esempio che mostra un form di login non sicuro.

ESEMPIO

In questo esempio utilizziamo un form non sicuro per l'immissione dei dati di login. Il form legge il nome utente e la password senza tuttavia cifrare quest'ultima:

```
<form action="verifica.php" method="post">
<p><label for='username'>Username</label>
<input type='text' name='utente'>
</p>
<p><label for='pwd'>Password</label>
<input type='text' name='password'>
</p>
<p><input type="submit" name="submit" value="Login">
</p>
</form>
```

Il codice mostra un form che richiama la pagina verifica.php. Cosa c'è di sbagliato in questo codice? Prima di tutto il campo pwd deve essere di "password" e non di tipo "text", in questo modo l'utente digitando la password come testo in chiaro sul display rischia che venga letta da occhi indiscreti. Questo problema è di facile soluzione, basta cambiare il tipo del campo in modo che venga visualizzata una serie di asterischi.
Adesso passiamo a vedere il codice del file verifica.php che elabora l'invio del modulo:

```
$user = $_POST['utente'];
$pw = $_POST['pwd'];
$sql = "SELECT user,password FROM users WHERE user='$user' AND password='$pw';
$result = mysql_query($sql);
if (mysql_num_rows($result))
{
//Codice eseguito se utente trovato
```

```
}
else
{
// Codice eseguito se utente NON trovato
}
```

In questo caso il rischio è quello di una SQL Injection, tecnica che consente di accedere alle informazioni del database mediante una "iniezione" di codice SQL in PHP.

L'SQL Injection è un particolare tipo di attacco il cui scopo è quello di indurre il database a eseguire query SQL non autorizzate. Consideriamo la seguente query:

```
SELECT * FROM Tabella WHERE username='$utente' AND password='$pwd'
```

`$user` e `$pass` sono impostate dall'utente e supponiamo che nessun controllo su di esse venga fatto. Tuttavia se inseriamo i valori seguenti:
`$utente` = ' or '1' = '1
`$pwd` = ' or '1' = '1
la query risultante sarà:

```
SELECT * FROM Tabella WHERE username='' or '1' = '1' AND password=''
or '1' = '1'
```

Il risultato è devastante: verranno identificati tutti gli utenti!

Per evitare il rischio di venire intercettati con SQL Injection, possiamo modificare la pagina php come segue:

```
$user = strip_tags(substr($_POST['user'],0,32));
$pw = strip_tags(substr($_POST['password'],0,32));
$sql = "SELECTuser,passwordFROM users WHERE user='". mysql_real_escape_
string($user)."'
AND password='". mysql_real_escape_string($pw)."';";
$result = mysql_query($sql);
if (mysql_num_rows($result))
{
//Codice eseguito se utente trovato
}
else
{
//Codice eseguito se utente NON trovato
}
```

In questo caso è stato effettuato un approccio blacklist: eliminando tutti i casi negativi. Come abbiamo visto l'origine di tutti i mali è rappresentata dall'apice singolo (')). Mediante la funzione `mysql_real_escape_string()` anteponiamo il carattere slash (/) davanti agli eventuali apici presenti nella stringa. Un altro problema è legato a stringhe troppo lunghe e potenzialmente dannose al sistema. Questo viene risolto tagliando la stringa a 32 caratteri (funzione `substr()`). Infine l'eliminazione di tag pericolosi viene effettuata da `strip_tags()` che toglie tutti i tag HTML inviati da malintenzionati utenti.

Tuttavia al termine di questo processo abbiamo ancora le password memorizzate in chiaro nel database: è necessario porre rimedio anche a questo: la soluzione più semplice è quella di effettuare una crittografia con la funzione `crypt()` di PHP.

La funzione crypt()

La funzione `crypt()` di PHP implementa la crittografia a senso unico (one way) o di hashing, una volta che, effettuata la crittografia, non possiamo tornare indietro al testo in chiaro. Questo si rende necessario per proteggere le informazioni, in quanto se l'elenco delle password cade nelle mani sbagliate, non c'è modo per ottenere il testo in chiaro.

La sintassi della funzione `crypt()` è la seguente:

```
stringcrypt (stringa,sale)
```

dove `stringa` è la stringa in input della funzione hash e `salt` (◀ sale ▶) è un parametro stringa opzionale che viene concatenato con la stringa per il calcolo dell'hash.

◀ Sale è una sequenza casuale di bit utilizzata assieme a una password come input a una funzione unidirezionale, di solito una funzione hash, il cui output è conservato al posto della sola password, e può essere usato per autenticare gli utenti. Usando dati sale si complicano gli attacchi a dizionario, quella classe di attacchi che sfruttano una precedente cifratura delle voci di un elenco di probabili parole chiave per confrontarle con l'originale: ogni bit di sale utilizzato raddoppia infatti la quantità di memorizzazione e di calcolo necessari all'attacco. ▶

Il sale è un parametro che viene utilizzato per aumentare la sicurezza dell'hash contro attacchi basati su dizionari. Se non specifichiamo nulla come parametro, PHP genera automaticamente una stringa casuale a ogni esecuzione della funzione.

La lunghezza del sale dipende dall'algoritmo utilizzato per il calcolo dell'hash che dipende a sua volta dal sistema operativo utilizzato. Vediamo un esempio d'utilizzo della funzione `crypt()`:

```
$password= "test";
//Ottengo l'impronta digitale in stringa
$stringa= crypt($password);
echo "Hash('".$password."')= ".$stringa;
```

Ogni volta che si esegue questo script il valore di `$stringa` cambia, vediamone l'esecuzione:

```
Hash('test')= $1$uE2.fX4.$16V4o0bp/Ac4Qs7f6/dTX0
Hash('test')= $1$6N5.Vn5.$Eal93ARXFw8Vw26PK.QfI1
Hash('test')= $1$SI4.z54.$j9.jmBTHM65bqdHHYz1ck/
Hash('test')= $1$4c4.5X0.$1aP/wZz0P5j7hR6uE4Oh51
```

I caratteri in rosso sono i sali generati automaticamente da PHP. La stringa iniziale `$1$` identifica che è stata usata la tecnica MD5.

L'elenco dei sali disponibili è il seguente:

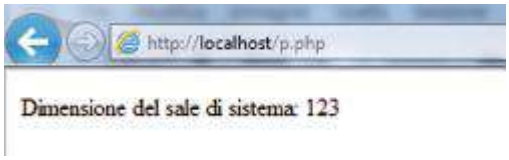
Algoritmo	Salt (sale)
CRYPT_STD_DES	2 caratteri (default)
CRYPT_EXT_DES	9 caratteri
CRYPT_MD5	12 caratteri, inizia con 1
CRYPT_BLOWFISH	16 caratteri, inizia con 2

Torniamo all'esempio della login visto in precedenza. Se pensiamo che la tabella degli utenti possa essere visionata da un amministratore di sistema, dobbiamo proteggere le password e le informazioni sensibili. Per fare questo prima di inserire il record di un utente nella tabella utenti, andremo a crittografarne la password mediante la funzione `crypt()`:

```
$user = strip_tags(substr($_POST['utente'],0,32));
$pw = strip_tags(substr($_POST['pwd'],0,32));
//La password viene crittografata
$cleanpw = crypt($pw);
//Inserimento record con password crittografata
$sql = "INSERT INTO users (username,password) VALUES('".mysql_real_escape_
string($user)."',
'".mysql_real_escape_string($cleanpw)."')";
//segue il resto del codice
```

Possiamo anche controllare l'impostazione del server con il seguente frammento di codice PHP:

```
<?php
echo "Dimensione del sale di sistema: ". CRYPT_SALT_LENGTH;
?>
```



Se vogliamo utilizzare l'algoritmo di crittografia MD5 dobbiamo indicarlo esplicitamente all'interno della funzione `crypt ()`. In questo modo qualunque stringa sarà trasformata in una stringa di lunghezza fissa di 32 caratteri. Vediamo l'esempio.

```
$user= strip_tags(substr($_POST['utente'],0,32));
$pw = strip_tags(substr($_POST['pwd'],0,32));
//Generazione password crittografata con algoritmo di hash MD5
$cleanpw = crypt(md5($pw),md5($user));
//Il resto del codice è uguale
```

Come facciamo per decodificare la stringa memorizzata nel database? Per fare questo usiamo il metodo di cifratura sulla password fornita dall'utente in ingresso per confrontarne il risultato con la password memorizzata nel database. Il codice che segue mostra quanto enunciato:

```
$user = strip_tags(substr($_POST['utente'],0,32));
$pw = strip_tags(substr($_POST['pwd'],0,32));
$cleanpw = crypt($pw,$user);
$sql = "SELECT user,passwordFROM users WHERE user='". mysql_real_escape_
string($user)."'
AND password='". mysql_real_escape_string($cleanpw)."';";
$result = mysql_query($sql);
if (mysql_num_rows($result))
{
//Codice eseguito se utente trovato
}
else
{
//Codice eseguito se utente NON trovato
}
```

Esiste un modo per conoscere la password? Sì, confrontando la stringa crittografata con una lunghissima lista di stringhe, una alla volta, fino a quando una partita è fatta. Questo metodo è chiama-

to attacco a dizionario, ed è questo uno dei motivi per il quale sarebbe bene non assegnare mai a una password un nome con senso logico, soprattutto se nome proprio o nome comune. Inoltre è bene assegnare alle password una lunghezza minima di almeno 8/9 caratteri e che contenga caratteri maiuscoli e minuscoli, numeri e caratteri speciali.

Zoom su...

UN USO POCO SICURO DELLA FUNZIONE CRYPT()

Esiste un metodo per l'utilizzo della funzione crypt (), molto diffuso, che tuttavia risulta insicuro. Si tratta di utilizzare come sale i primi *n* caratteri del testo in chiaro. Vediamo il codice di esempio.

```
$user = strip_tags(substr($_POST['utente'],0,32));
$pw = strip_tags(substr($_POST['pwd'],0,32));
$cleanpw =crypt($pw, substr($user,0,2));
$sql = "SELECT user,passwordFROM usersWHERE user='". mysql_real_escape_
string($user)."'
AND password='". mysql_real_escape_string($cleanpw)."' ;";
$result = mysql_query($sql);
if (mysql_num_rows($result))
{
 // Codice eseguito se utente trovato
}
else
{
//Codice eseguito se utente NON trovato
}
?>
```

Se ad esempio il nome utente è `rmarelli`, al sale viene anteposta la sottostringa `"rm"`, che rende più facile l'individuazione della stessa da un utente malintenzionato.

ESEMPIO

Criptare e decriptare con PHP per Linux

In questo esempio vogliamo inviare un messaggio fornendo poi un mezzo per decifrarlo. Per fare questo utilizzeremo una crittografia a chiave pubblica, supportata da PHP.
Per effettuare una crittografia asimmetrica a chiave pubblica è necessario che il mittente e il destinatario, cioè gli utenti, possiedano sia una chiave privata che una chiave pubblica; le chiavi pubbliche sono condivise con gli altri utenti. Se ad esempio desideriamo inviare un messaggio a un amico dobbiamo crittografarlo con una chiave pubblica, mentre invece lui per decifrarlo userà la sua chiave privata.

> La chiave pubblica e la chiave privata per ogni utente non sono matematicamente correlate. Attraverso PGP (PrettyGood Privacy) o altri metodi di crittografia a chiave pubblica, non c'è modo di ottenere o dedurre in nessun modo la chiave privata di qualcuno a partire dalla chiave pubblica.

Una caratteristica di PGP è che la password che rappresenta la chiave privata è in realtà una ◀ passphrase ▶.

> ◀ Una passphrase rappresenta una particolare password che può contenere anche più parole o stringhe alfanumeriche, incluso lo spazio. Il nome deriva dall'unione dei termini inglesi password e phrase ed è traducibile come frase di accesso o frase chiave. Può essere rappresentata da un intero proverbio, inclusi tutti i simboli di punteggiatura. ▶

Un metodo che consente di usare la crittografia a chiave pubblica (PGP-based) è quello di usare GNUPrivacyGuard (GPG) per Linux. Tutti i messaggi crittografati utilizzando GPG possono essere decifrati con GPG, PGP, con qualunque client di posta elettronica che supporti entrambi i programmi. In questo esempio l'utente compila un form che contiene il testo del messaggio da inviare, quindi effettua la crittografa dello stesso e lo invia a un destinatario utilizzando il programma gpg.

```
//Inserimento del mittente e destinatario
$mitt = "io@esempio.com";
$dest = "tu@esempio.com";
//Riduzione della lunghezza del messaggio rimozione tag HTML
//Messaggio ricevuto è il campo POST msg
$messagebody = strip_tags(substr($_POST['msg'],0,5000));
$message_body = escapeshellarg($messagebody);
//Percorso del programma sul nostro server
$gpg_path = '/usr/local/bin/gpg';
//Directory document root del server Apache
$home_dir = '/htdocs/www';
$user_env = 'web';
//Messaggio in codice Linux
$cmd = "echo $message_body | HOME=$home_dir USER=$user_env $gpg_path" .
"--quiet --no-secmem-warning --encrypt --sign --armor " .
"--recipient $dest --local-user $mitt";
$message_body = '$cmd';
//Ianciodella mail
mail($dest,'Message from Web Form', $message_body,"From:$mitt\r\n");
```

In questo esempio PHP manda in esecuzione il programma GNU GPG con il comando `/usr/local/bin/gpg`, tuttavia il percorso potrebbe variare in funzione di come abbiamo installato il pacchetto. Il programma effettua la crittografia del messaggio utilizzando la chiave privata del mittente e la chiave pubblica del destinatario. In effetti, solo il destinatario può decifrare il messaggio con la certezza che il messaggio proviene dal mittente.
Il comando inviato nel corpo del messaggio contiene alcuni comandi che effettuano le seguenti operazioni:

- `--quiet` e `--no-secmem-warning` servono per sopprimere i warning da gpg;
- `--encrypt` esegue la crittografia;
- `--sign` aggiunge una firma per verificare l'identità del mittente;
- `--armor` produce un output ASCII che può essere facilmente inviato via email.

Normalmente, e come detto, le chiavi segrete sono protette da una passphrase. Questo particolare esempio non usa una frase, altrimenti dovremmo inserirla manualmente su ciascun modulo di presentazione.

Se non usiamo una connessione con protocollo SSL il messaggio di posta elettronica inserito dall'utente nel form e inviato al server è completamente in chiaro: è visibile a chiunque nel tragitto tra il computer client e il server.

Prova adesso!

- Usare GNUGPG
- Usare PHP

Completa l'esempio aggiungendo il form che consente di far inserire il messaggio, l'indirizzo del mittente e del destinatario con un form usando postback.

Esercitazioni di Laboratorio 4

CRITTOGRAFIA IN PHP CON ALGORITMO BLOWFISH

PHP e Blowfish

In questo esempio vogliamo utilizzare l'algoritmo ◀ Blowfish ▶ per cifrare un testo in chiaro.

◀ Blowfish è un algoritmo a chiave simmetrica a blocchi, ideato nel 1993 da Bruce Schneier e implementato in molti software di crittografia. Quest'algoritmo utilizza varie tecniche tra le quali la rete Feistel, le S-box dipendenti da chiavi e funzioni F non invertibili che lo rendono, forse, l'algoritmo più sicuro attualmente disponibile. Le chiavi utilizzate sono di dimensioni variabili fino a un massimo di 448 bit e i blocchi utilizzati per la cifratura sono di 64 bit. Non si conoscono al momento tecniche di attacco valide nei suoi confronti. È considerato uno degli algoritmi di cifratura a blocchi più veloce ed è di pubblico dominio. ▶

Vogliamo creare una classe che, dopo aver incluso il codice che esegue le operazioni tipiche dell'algoritmo, fornisca dei metodi utili a eseguire le seguenti operazioni:

- impostare la chiave;
- codificare una stringa;
- decodificare una stringa.

L'esempio è contenuto nella sotto directory crittografia e si compone dei seguenti file:

`index.html`
mostra il form che consente di leggere il testo da criptare e mostrare i risultati;

`cripto.php`
è lo script che contiene la classe Cifratura e che include la pagina dell'algoritmo Blowfish (`blowfish.php`);

`blowfish.php`
contiene l'intero algoritmo di cifratura;

`prova.php`
è lo script che effettua la cifratura e la decifratura.

Iniziamo a vedere il codice della classe Crittografia. Come possiamo notare possiede due proprietà: `$chiave` e `$blowfish` che rappresentano rispettivamente la chiave e il testo codificato.

Siccome la classe Crittografia impiega i metodi dell'algoritmo Blowfish, è necessario includerne il codice (riga 4).

Il costruttore della classe (righe 13-16) riceve come parametro una stringa che sarà la chiave utilizzata per la cifratura e la decifratura. Il metodo cifratura (righe 19-32) riceve come parametro una stringa e restituisce una nuova stringa che è rappresentata dal testo cifrato. Per fare questo viene istanziato l'oggetto `Horde_Cipher_blowfish` (riga 20) e viene suddivisa la stringa di input in gruppi di 8 caratteri per effettuare la cifratura un blocco alla volta (righe 22-31).

```
1  <?php
2  //Richiamo il codice che coniene tutti i metodi e le classi necessari
3  //per utilizzare Blowfish
4  require_once('blowfish.php');
5  //Definizione della classe
6  class Crittografia
7  {
8      //Proprietà
9      var $chiave;
10     var $blowfish;
11     //Costruttore della classe Crittografia
12     //Riceve come argomento la chiave in chiaro
13     function Crittografia($str)
14     {
15         $this->chiave = $str;
16     }
17     //Metodo che codifica la stringa originale
18     function cifratura($str)
19     {
20         $this->blowfish = new Horde_Cipher_blowfish;
21         $encrypt = '';
22         $mod = strlen($str) % 8;
23         if ($mod > 0)
24         {
25             $str.=str_repeat("\0",8-$mod);
26         }
27         foreach (str_split($str,8) as $chunk)
28         {
29             $encrypt .= $this->blowfish->encryptBlock($chunk, $this->getChiave());
30         }
31         return base64_encode($encrypt);
32     }
33     //Metodo che decodifica la stringa criptata
```

Il metodo decifratura funziona in modo analogo al metodo cifratura, con la sola differenza che restituisce il testo in chiaro.

```
34     function decifratura($str)
35     {
36         $this->blowfish = new Horde_Cipher_blowfish;
37         $decrypt = '';
38         $data = base64_decode($str);
39         foreach (str_split( $data, 8 ) as $chunk)
40         {
41             $decrypt .= $this->blowfish->decryptBlock($chunk, $this->getChiave());
42         }
43         return trim($decrypt);
44     }
45     //Metodo che restituisce la chiave
46     function getChiave()
47     {
48         return $this->chiave;
49     }
50 }
51 ?>
```

Vediamo il codice della pagina prova.php. Innanzitutto viene incluso il codice della pagina `cripto.php` (riga 3) che contiene i metodi necessari al criptaggio e decriptaggio della frase. Dopo aver letto i campi POST ricevuti dal form presente nella pagina index.html e salvato nelle variabili `$chiave` e `$txt` (righe 5-6) viene istanziato un oggetto di classe Crittografia chiamato `$blowfish` (riga 8). A quel punto viene invocato il metodo cifratura (riga 10) e quindi decifratura (riga 13) per restituire alla pagina index.html il testo criptato e decriptato.

```
1  <?php
2  //Inclusione classe Crittografia presente nel file cripto.php
3  require_once 'cripto.php';
4  //Lettura campi POST dal form di index,html
5  $chiave = $_GET['chiave'];
6  $txt = $_GET['stringa'];
7  //Istanza di un oggetto $blowfish di classe Crittografia
8  $blowfish = new Crittografia($chiave);
9  //Invocazione metodo cifratura per ottenere il testo cifrato
10 $txt_cifrato = $blowfish->cifratura($txt);
11 //Stampa risultati
12 echo "Testo cifrato:<BR>".$txt_cifrato."<BR><HR>";
13 echo "Testo decifrato:<BR>".$blowfish->decifratura($txt_cifrato)."";
14 ?>
```

Infine il codice della pagina index.html si commenta da solo, è formato da una funzione (righe 6-28) che istanzia l'oggetto di Ajax per fare in modo che il testo inserito dall'utente venga inviato alla pagina di elaborazione (prova.php) senza chiudere la pagina HTML. La funzione `MyHandler()` viene richiamata dall'evento `onreadystatechange`, e gestisce la risposta del server (righe 30-39).

```
1  <HTML>
2  <HEAD>
3  <SCRIPT TYPE='text/javascript'>
4  var myRequest = null;
5  //Creazione oggetto Ajax
6  function CreateXmlHttpReq(handler)
7  {
8     var xmlhttp = null;
9     try
10    {
11       xmlhttp = new XMLHttpRequest();
12    }
13    catch(e)
14    {
15       try
16       {
17          xmlhttp = new ActiveXObject("Msxml2.XMLHTTP");
18       }
19       catch(e)
20       {
21          xmlhttp = new ActiveXObject("Microsoft.XMLHTTP");
22       }
23    }
24    //Dopo una richiesta al server, serve una funzione che possa ricevere i dati restituiti dal server.
25    //onreadystatechange contiene la funzione che processerà la risposta del server.
26    xmlhttp.onreadystatechange = handler;
27    return xmlhttp;
28 }
29 //Funzione che viene eseguita da onreadystatechange
30 function myHandler()
31 {
32    //readyState contiene lo stato della response del server. Ogni volta che readyState cambia,
33    //la funzione onreadystatechange viene eseguita
34    if (myRequest.readyState == 4 && myRequest.status == 200)
35    {
36       e = document.getElementById('testo');
37       e.innerHTML = myRequest.responseText;
38    }
39 }
```

La funzione `Cifra()` è attivata al clic sul form, dopo aver immesso la parola da criptare e la chiave di criptaggio. Dopo aver letto i campi del form (righe 44-45), richiama la funzione `CreateXmlHttpReq()` (riga 49) associando a essa la funzione `myHandler` vista in precedenza. Il metodo `open` e `send` di Ajax completano (righe 53-56) la funzione.

```
40  //Funzione attivata al click sull'invio del form
41  function Cifra()
42  {
43     //lettura valori dal form
44     var chiave = document.modulo.chiave.value;
45     var testo = document.modulo.stringa.value;
46     //I dati trasmessi dal server sono ricevuti da responseText di tipo di stringa e inseriti nel div 'testo'
47     document.getElementById('testo').innerHTML="<SPAN STYLE='color:red'>Attendere elaborazione...</SPAN>";
48     //Creazione oggetto Ajax
49     myRequest = CreateXmlHttpReq(myHandler);
50     //3 parametri: Il primo definisce quale metodo usare (GET/POST)
51     //Il secondo è l'url dove risiede lo script server-side
52     //Il terzo (booleano) specifica che la richiesta deve essere asincrona
53     myRequest.open("GET","prova.php?chiave="+escape(chiave)+"&stringa="+escape(testo),true);
54     //Trasmette effettivamente la richiesta al server. Il parametro nullo indica POST
55     //per GET mettere i parametri tra parentesi
56     myRequest.send(null);
57  }
58  </SCRIPT>
59  </HEAD>
60  <BODY>
61  <TABLE><TR><TD>
62  <FORM METHOD='get' NAME='modulo'>
63  Chiave: <TD><INPUT TYPE='text' SIZE='10' NAME='chiave'>
64  <TR><TD colspan=2>Testo da cifrare:<TR><TD colspan=2><TEXTAREA NAME='stringa' ROWS='4' COLS='50'></TEXTAREA>
65  <TR><TD><INPUT TYPE='button' VALUE='Codifica' onClick='Cifra()'>
66  </FORM></TABLE>
67  <DIV ID='testo'></DIV>
68  </BODY>
69  </HTML>
```

L'esecuzione mostra la parola che viene codificata e quindi decodificata: ▶

Prova adesso!

- Utilizzare le classi di Blowfish
- Crittografare e decrittografare messaggi

APRI IL FILE index.html, prova.php, cripto.php

Modifica lo script degli esempi proposti in modo tale da inviare messaggi criptati tra due host in rete.

Esercitazioni di Laboratorio 5

CREAZIONE DI VOLUMI CRIPTATI CON VERACRYPT

VeraCrypt

◀ VeraCrypt ▶ è un software che non serve per criptare un singolo file ma un intero volume, rientra quindi nella categoria dei programmi di tipo Disk Encryption.

◀ È un software completamente gratuito e open source per la cifratura, derivato completamente da TrueCrypt, famosissimo programma multi-piattaforma il cui sviluppo è cessato nel 2014. ▶

I file vengono decifrati automaticamente al volo (on the fly) mentre vengono letti o copiati da un volume VeraCrypt criptato nella RAM e, allo stesso modo, vengono scritti o copiati nel volume VeraCrypt dopo la loro codifica: non è richiesta memoria aggiuntiva per eseguire queste operazione dato che non è necessario che l'intero file da criptare/decriptare sia completamente caricato in memoria RAM.

Installazione di VeraCrypt

1. Per prima cosa è necessario scaricare l'ultima versione di VeraCrypt dal sito: http://sourceforge.net/projects/veracrypt dopo aver fatto clic su Download otteniamo il file di installazione:

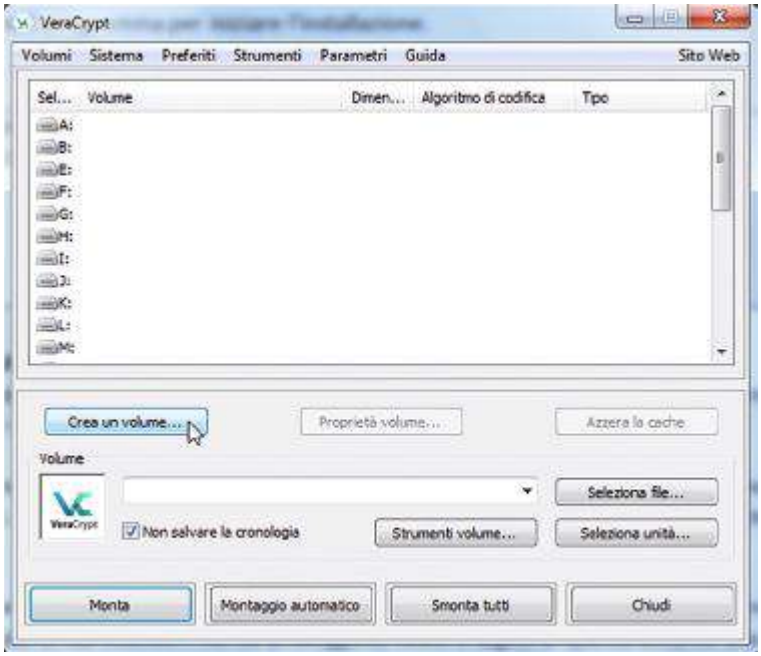
2. Quindi avviamo il programma per iniziare l'installazione.
3. Dopo aver fatto confermato l'accettazione della licenza, fatto clic su Install, scelto la directory di installazione ecc., otteniamo la seguente icona per avviare il programma:

Creare il volume criptato

Dopo aver completato l'installazione del programma, passiamo alla creazione di un volume cifrato. In seguito potremo ad esempio proteggere una cartella con password.

Prima di tutto può essere utile attivare la lingua italiana. Per fare questo facciamo clic sul menu Settings, quindi Language, selezioniamo poi la voce Italiano nella finestra che si apre, e infine OK per confermare.

1. Dopo aver aperto il programma facciamo clic sul pulsante Crea un volume per avviare la creazione del nostro archivio cifrato.



2 Mettiamo quindi il segno di spunta accanto alla voce Crea un file contenitore criptato e clicchiamo su Avanti per continuare:

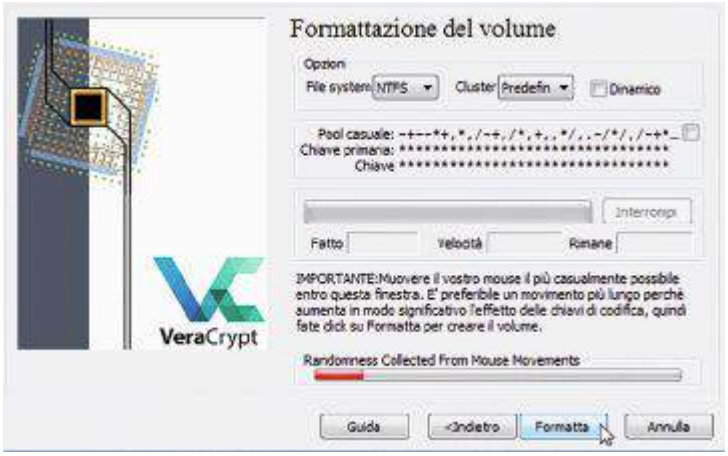
3 Adesso dobbiamo indicare se la partizione da creare deve essere nascosta. Selezionando l'opzione Volume VeraCrypt nascosto viene creata una partizione nascosta, la cui esistenza non può nemmeno essere dimostrata. In questo caso procediamo selezionando l'opzione Volume VeraCrypt standard, quindi facciamo clic su Avanti:

4. Nella schermata successiva dobbiamo indicare il nome e il percorso in cui creare il file da utilizzare come contenitore della partizione cifrata: nel nostro caso assegniamo a esso il nome enigma , lo memorizziamo nel volume C:, quindi facciamo clic su Salva e infine proseguiamo facendo clic su Avanti.
5. Adesso dobbiamo selezionare l'algoritmo di cifratura da utilizzare per il nostro volume. Lasciamo attiva l'impostazione predefinita: AES in corrispondenza della sezione Algoritmo di codifica e SHA–512 in corrispondenza della sezione Algoritmo di confusione. Facciamo clic su Avanti.

I volumi VeraCrypt possono essere crittografati utilizzando i seguenti algoritmi:

Algoritmo	Key Size	Block Size
AES	256	128
Serpent	256	128
Twofish	256	128
AES-Twofish	256; 256	128
AES-Twofish-Serpent	256; 256; 256	128
Serpent-AES	256; 256	128
Serpent-Twofish-AES	256; 256; 256	128
Twofish-Serpent	256; 256	128

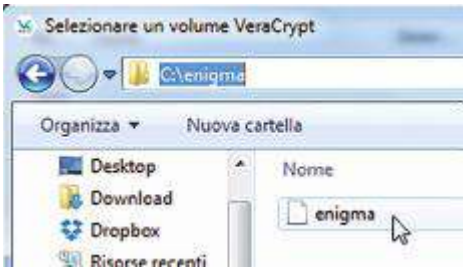
6. A questo punto dobbiamo selezionare il limite massimo di spazio per il volume cifrato, quindi facciamo clic sul pulsante Avanti.
7. Ora dobbiamo stabilire la password che deve essere sicura, cioè composta sia da caratteri minuscoli che maiuscoli, numeri e caratteri speciali (?,/, !, £, &, $, (,), .), quindi facciamo clic sul pulsante Avanti.
8. L'ultimo passaggio ci consente di selezionare il file system da utilizzare per il volume cifrato appena creato. Per poter memorizzare nel volume cifrato archivi molto corposi (oltre i 2 GB), scegliamo NTFS, altrimenti lasciamo l'impostazione FAT. Quindi facciamo clic su Formatta per far partire la formattazione. Infine premiamo OK e quindi su Esci.
Quando la procedura è terminata è possibile iniziare a utilizzare l'hard disk virtuale cifrato. ▼



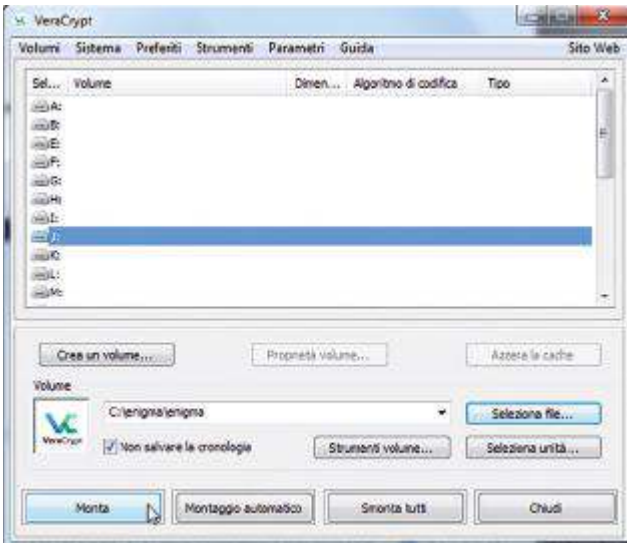
Montare/smontare il disco VeraCrypt

Ogni volta che si desidera utilizzare il disco virtuale creato con VeraCrypt è necessario prima di tutto montarlo per averlo a disposizione come unità logica di sistema.

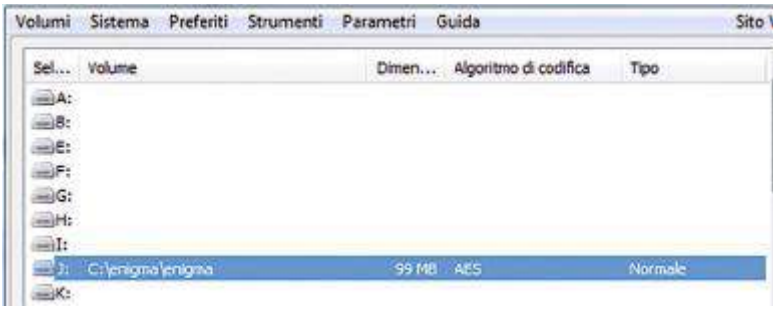
1. Per fare questo facciamo clic su Seleziona File nella schermata principale e ricerchiamo il file salvato in precedenza, in questo caso disco C:\enigma: ▶



2. Quindi facciamo clic sul pulsante Monta, scegliendo l'unità logica da associare, in questo caso J: ▼



3. Ci viene quindi richiesta la password di accesso impostata durante la creazione. Dopo averla inserita e confermato tutto con OK, otteniamo: ▼



4. Come possiamo notare viene creato un nuovo volume, rappresentato da un'unità logica, in questo caso J:.

Al termine delle operazioni, per evitare che qualcuno possa accedere abusivamente al nostro hard disk virtuale, prima di chiudere VeraCrypt è necessario procedere a smontare il disco cliccando su Smonta tutti presente nella schermata principale del programma.

Prova adesso!

- Utilizzare il pacchetto VeraCrypt

Dopo aver installato il pacchetto e creato due dischi virtuali criptati, modifica la password utilizzando le opzioni presenti nel menu Sistema: quindi effettua un test comparativo tra gli algoritmi utilizzando l'apposito programma presente nel menu Strumenti, modificando volta per volta la dimensione del buffer: quali sono le tue osservazioni? Per ciascuno dei metodi crittografici utilizzati dal programma (ed elencati nella precedente schermata) scrivi le caratteristiche fondamentali e produci una tabella che ne permetta la loro comparazione.

Esercitazioni di Laboratorio 6

LA FIRMA DIGITALE CON LA CARTA CNS-TS

Informazioni sulla firma digitale

La firma elettronica è stata introdotta nella normativa europea dalla Direttiva 1999/93/CE. La validità e l'utilizzo della firma elettronica nell'ordinamento italiano sono disciplinate dal decreto legislativo 7 marzo 2005, n. 82, il cosiddetto "Codice dell'amministrazione digitale", modificato dal d.lgs. 4 aprile 2006, n. 159.

Un documento con firma digitale consente di risalire con certezza all'identità del firmatario, e consente di riconoscere se il documento stesso è stato modificato o meno dopo l'apposizione della firma. La firma digitale può essere apposta solo utilizzando un dispositivo (smartcard o "chiavetta" USB) rilasciato da appositi enti certificatori, i quali accertano l'identità del richiedente prima di consegnargli la carta.

La firma digitale in formato p7m consente di firmare qualunque tipo di file (rtf, doc, tiff, xls, pdf ecc.). Durante l'apposizione della firma il file viene "incapsulato" in una "busta crittografica", e il risultato è un nuovo file, con estensione .p7m. L'identità del firmatario e la validità della firma apposta nel file p7m possono essere verificate con i sw forniti dagli enti di certificazione, oppure mediante servizi online (p. es. http://ca.notariato.it/). Con questi stessi strumenti, dalla "capsula" p7m può essere estratto il file ivi contenuto, che tornerà a essere nel formato originario, non più dotato di firma e quindi visualizzabile e modificabile con l'applicazione utilizzata per crearlo.

La firma digitale in formato pdf è applicabile ai soli file pdf. In questo caso non viene effettuato un "incapsulamento" ma la firma viene inserita direttamente all'interno del file, che quindi rimane in formato pdf e può essere aperto e visualizzato direttamente con una applicazione che gestisca i file pdf. La verifica della firma può essere effettuata mediante il sw Adobe Reader o mediante altri sw dotati di funzionalità analoghe.

È bene ricordare che, in entrambi i casi, il documento originale, contenente la firma, è quello informatico, e non esiste un originale firmato con la penna. La riproduzione a stampa del file è quindi da considerarsi una copia, ovvero mera "riproduzione meccanica" dell'originale avente lo stesso valore di una fotocopia cartacea di un documento originale cartaceo.

La firma digitale è un'operazione con la quale si genera un codice crittografico che dimostra l'identità e l'integrità di un documento. In altre parole, la firma digitale permette di verificare che il documento:
- è stato firmato da una ben precisa persona;
- successivamente, non ha subito modifiche.

La firma digitale si basa su algoritmi crittografici che richiedono il possesso, da parte dell'utente, di una chiave privata e di un corrispondente certificato. La chiave privata e il certificato sono normalmente memorizzati su un dispositivo elettronico simile a una carta di credito, chiamato smartcard, oppure su un token USB (in entrambi i casi si tratta di microchip con funzionalità crittografiche):

In fase di generazione della firma, è necessario digitare il PIN della propria smartcard o dispositivo USB.
Il certificato è un piccolo file contenente informazioni essenziali per la verifica della firma, e cioè:
- il nome e il codice fiscale dell'utente titolare (es. Mario Rossi);
- il nome dell'azienda di appartenenza, se applicabile;
- il nome dell'ente certificatore;
- la data di inizio e la data di fine validità;
- la chiave pubblica del titolare;
- altre informazioni di servizio.

Il certificato viene rilasciato all'utente da un ente terzo fidato, detto certificatore (Certification Authority, CA).
Dopo aver generato una firma digitale, questa viene solitamente salvata in un file detto busta crittografica; la busta contiene normalmente anche il documento di partenza e il certificato del firmatario, così da tenere insieme tutte le informazioni necessarie per la verifica.
Esistono diversi formati di busta crittografica; il più diffuso è quello conosciuto come PKCS#7 (in tal caso il file ha l'estensione P7M), che è quello riconosciuto dalla PA.
Affinché la firma digitale abbia un pieno valore legale (in tal caso si parla di firma qualificata), devono essere rispettate diverse norme di legge che stabiliscono requisiti relativi alle chiavi, al certificato, alla smartcard, al certificatore, al formato della busta crittografica ecc.

Cos'è la CNS e a cosa serve?

La Carta Nazionale dei Servizi o CNS è una Smart Card (o una Pen drive) che contiene un "certificato digitale" di autenticazione personale. È uno strumento informatico che consente l'identificazione certa dell'utente in rete e permette di consultare i dati personali resi disponibili dalle pubbliche amministrazioni direttamente su sito Web, come ad esempio, l'accesso ai referti medici sul sito Web della propria ASL (Tessera Sanitaria sia nazionale che europea). La CNS rilasciata dalle Camere di Commercio è un dispositivo integrato che consente, a chi ha una carica all'interno di un'impresa, di firmare digitalmente documenti informatici (bilanci, fatture, contratti ecc.) e di accedere in rete ai servizi della Pubblica Amministrazione.

Inoltre consente, al legale rappresentante di un'impresa, di consultare gratuitamente le informazioni relative alla propria azienda contenute nel Registro Imprese:
- visura ordinaria, visura storica, visura artigiana e scheda società;
- modello di dichiarazione sostitutiva del certificato Registro Imprese;
- statuti, atti e bilanci depositati;
- situazione dei pagamenti del diritto annuale;
- stato pratiche Registro Imprese (trasparenza amministrativa).

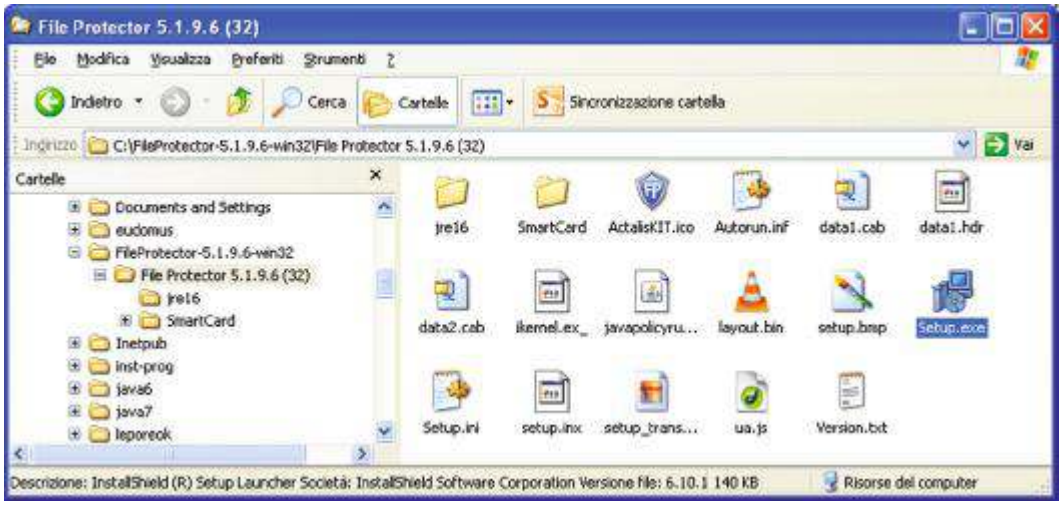
Con la CNS rilasciata dalle Camere di Commercio, è possibile inoltre, come privati cittadini, collegarsi via Internet al sito dell'Agenzia delle Entrate (http://telematici.agenziaentrate.gov.it), registrarsi senza dover digitare tutti i propri dati e accedere così al sito per verificare lo stato della propria posizione fiscale (condoni e concordati, versamenti, richieste di variazione di posizione, rimborsi, registrazione contratti di locazione di beni immobili, comunicazioni relative ai regimi fiscali agevolati e altro).
Il certificato digitale contenuto all'interno della CNS è l'equivalente elettronico di un documento d'identità (come il passaporto o la carta d'identità) e identifica in maniera digitale una persona fisica o un'entità. Viene emesso da un'apposita Autorità di certificazione (Certification Authority, CA) riconosciuta secondo standard internazionali, la quale garantisce la validità delle informazioni riportate nel certificato. Come i documenti cartacei, anche il certificato digitale ha una validità temporale al di fuori della quale risulterà scaduto.

File protector

Un pacchetto gratuito che ci permette di firmare e cifrare i documenti utilizzando la CNS è File Protector, scaricabile all'indirizzo: http://www.card.infocamere.it/infocamere/pub/download-sw-firma_3177 dopo aver scelto la versione adatta al proprio sistema operativo.

Una volta terminato il download è necessario decomprimere il file in una cartella, ad esempio quella con nome proposto automaticamente cliccando sul file zippato col tasto destro del mouse: ▶

Avviamo l'istallazione cliccando sul file setup.exe:

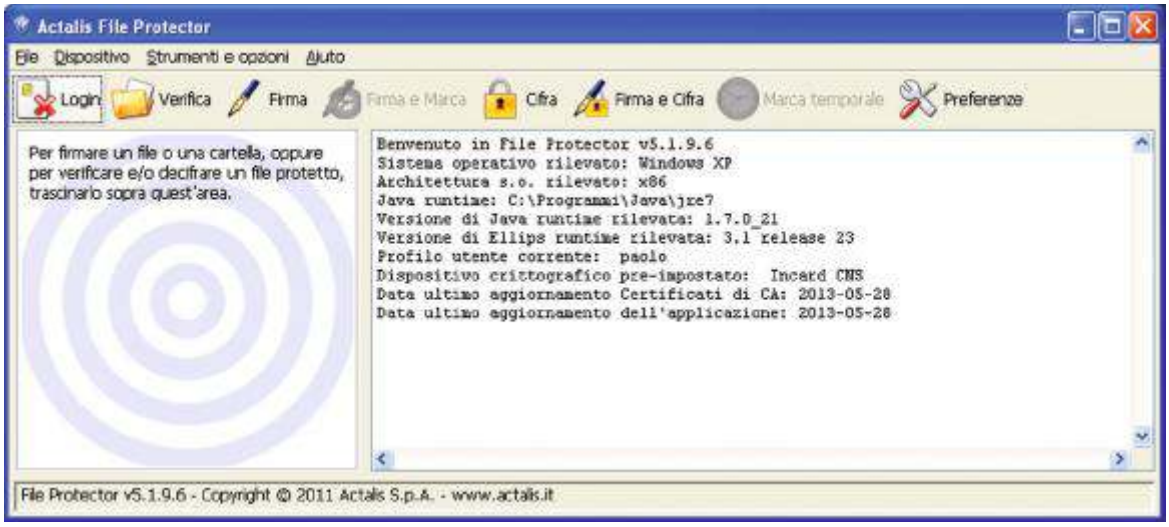


Dopo aver lanciato il file setup.exe sarà avviata l'installazione automatica: è necessario seguire le indicazioni riportate a video avendo cura di selezionare la modalità di installazione COMPLETA.
Al termine dell'installazione sarà necessario inserire la carta nel lettore e sarà possibile utilizzare il software per l'utilizzo della CNS e la Firma digitale.

Dopo aver riavviato il computer avviamo l'applicazione tramite l'icona.

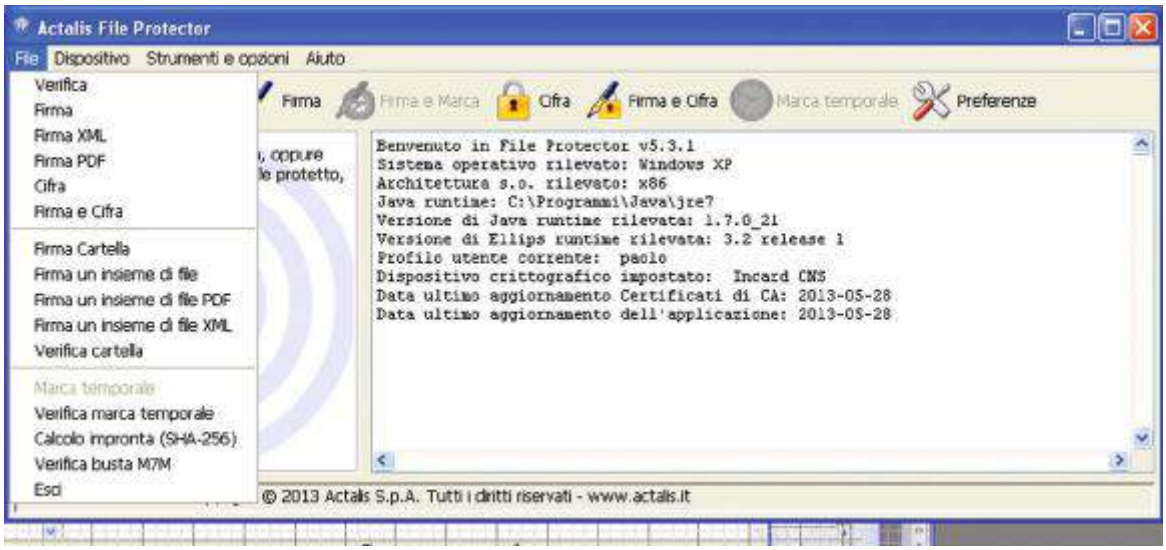
Ci viene richiesta la definizione di un profilo utente per poter iniziare le operazioni di firma: ▶

Dopo aver creato un profilo (inserendo una password di almeno 6 caratteri), viene visualizzato il menu generale:



Per poter procedere, dopo aver inserito la card nel lettore, è necessario effettuare la login, inserendo il PIN della carta CNS: ▶

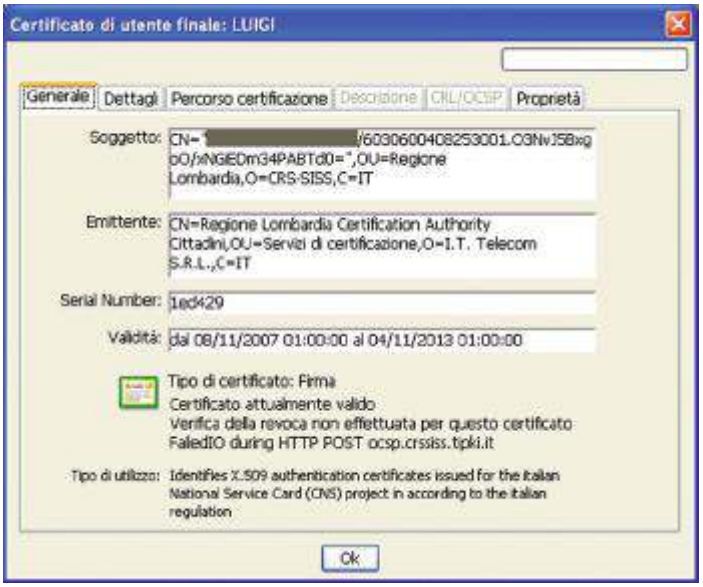
Nella prima tendina sono elencate tutte le possibili operazioni effettuabili con File Protector, dalla semplice firma alla verifica della busta M7M:



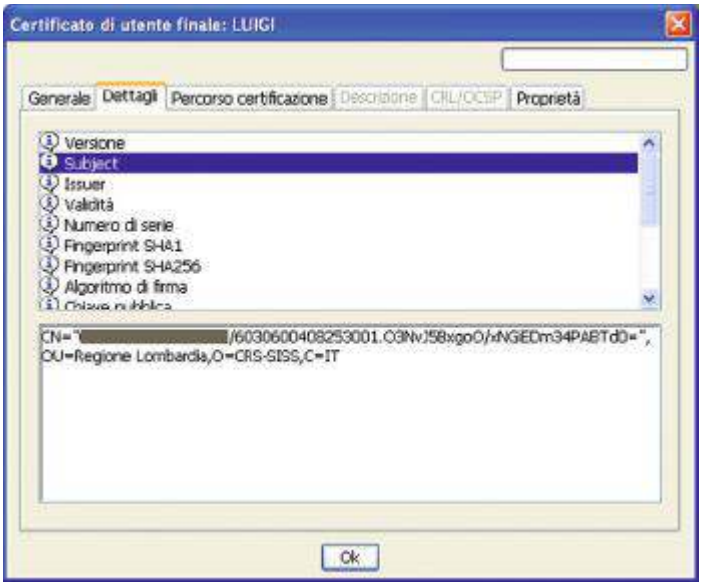
Nella seconda tendina del menu, oltre alle opzioni di configurazione, è possibile visualizzare l'elenco dei certificati disponibili:

Selezioniamo quello che ci viene proposto, dato che sulla CNS è presente generalmente un solo certificato: ▶

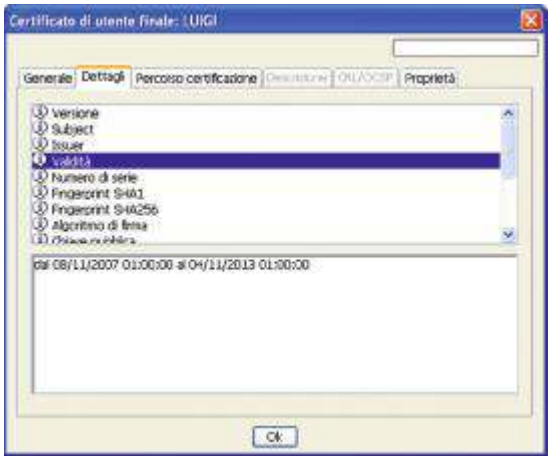
Nella prima parte del certificato, nella finestra generale, sono presenti appunto i dati generali del certificato, cioè chi lo ha emesso, quando scade e il suo numero di serie: ▶



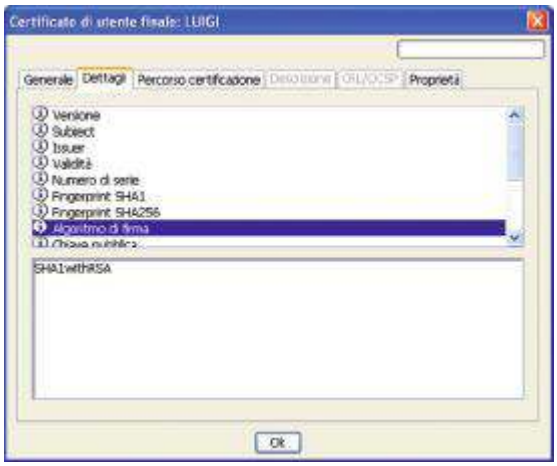
Nella seconda sezione si possono vedere tutti i dettagli, cioè gli attributi e le caratteristiche del certificato, tra cui il soggetto già riportato tra i dati generali: ▶



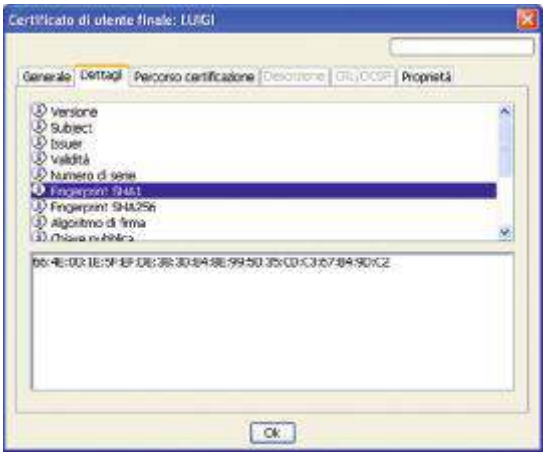
il periodo di validità del certificato: ▼



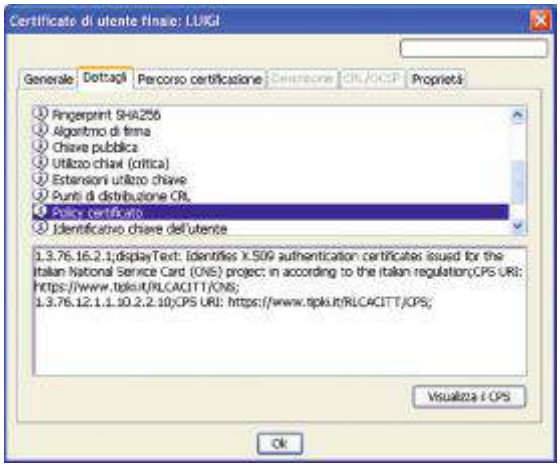
l'algoritmo di firma, che nel nostro caso è il SHA con RSA: ▼



l'impronta digitale sia nel formato SHA1 che SHA256: ▼

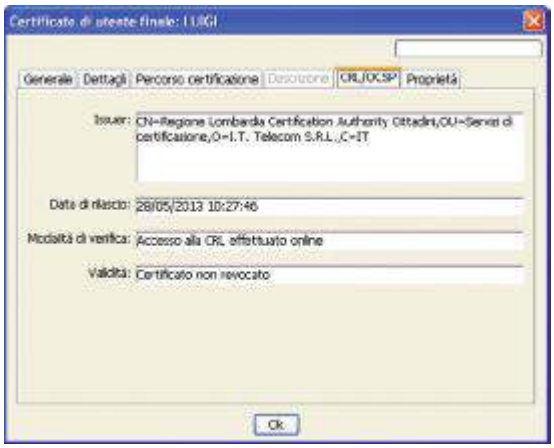


i dati di riferimento alla policy del certificato, incluso l'indirizzo nel quale poter verificare l'autenticità e la validità del certificato e la verifica della eventuale revoca: ▼

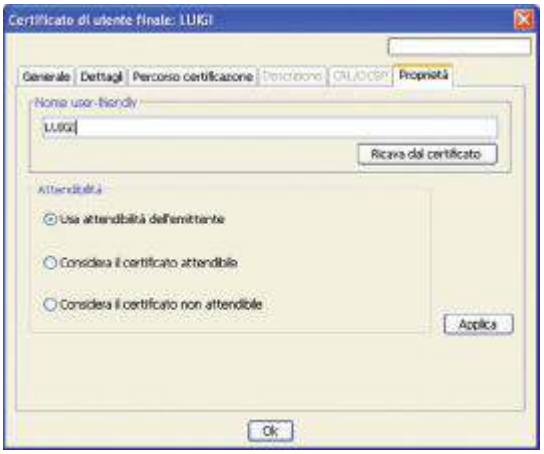


◀ Nella schermata a fianco è presente l'albero dei certificatori, che in questo caso si riduce a un solo livello dato che è stato emesso dalla root "*Regione Lombardia Certification Authority*".

Se il certificato viene verificato online si abilita anche la successiva finestra, che contiene i dati del certificatore: ▼



Nell'ultima videata viene richiesto di scegliere la modalità di verifica del certificato ed è possibile inoltre modificare il nome del certificato, in modo da utilizzarlo più comodamente nelle operazioni successive: ▼



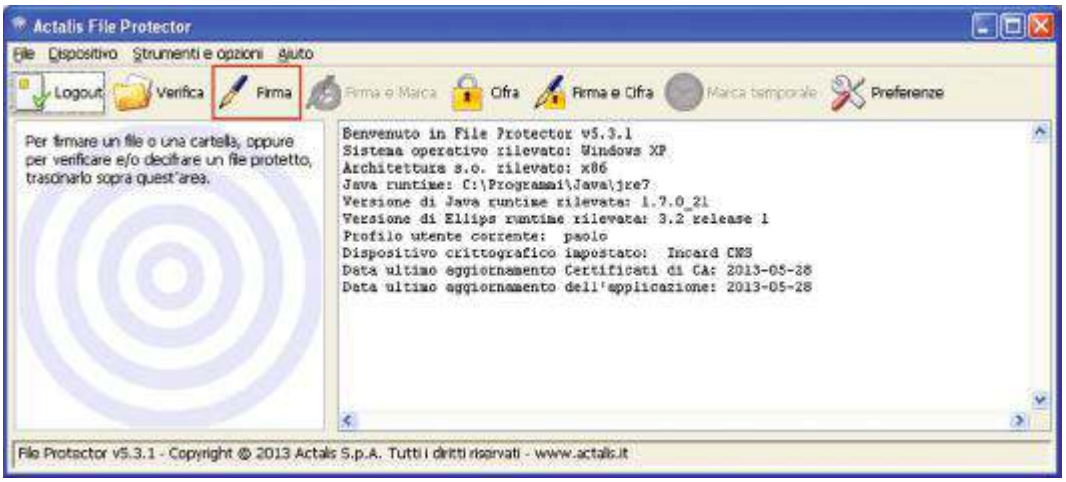
Nel caso che il certificato del firmatario non sia presente nel database ne viene proposto l'inserimento con la seguente videata: ▶

Dopo che viene visualizzato il certificato dell'ente certificatore è possibile aggiungerlo all'archivio personale: ▶

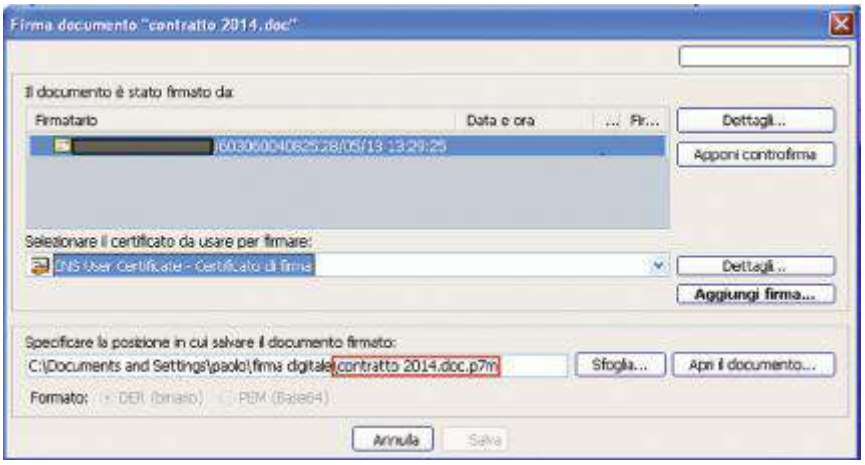
Nella terza finestra possiamo visualizzare il database completo dei certificati:

Alla prima connessione è probabilmente vuoto, ma effettuando l'importazione dal server LDAP otteniamo il seguente elenco: ▶

Procediamo ora con la procedura di firma di un documento, ad esempio il file contratto 2014.doc, cliccando direttamente sull'icona Firma: ▶



È necessario scegliere sia il *firmatario* che il *certificato* che deve essere utilizzato per apporre la firma digitale: ▶



Una volta individuato il file questo verrà trasformato in un nuovo documento con suffisso p7m e avrà la seguente icona:

Analogo procedimento è previsto per cifrare il documento:

Dopo aver selezionato il destinatario è possibile cifrare il file sia nel suo formato originale .doc. ottenendo un file .doc.p7e: ▶

oppure partendo dal file già firmato in precedenza in modo da ottenere il file .doc.p7m.p7e:

Nella cartella sarà ora presente un nuovo file con la seguente icona:

Prova adesso!

- Applicare la firma digitale alla CNS

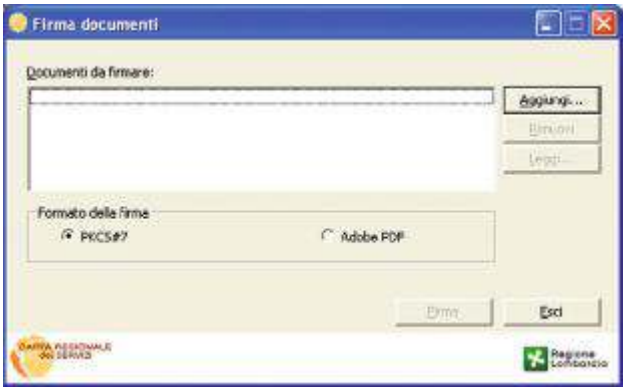
Dopo aver scaricato e installato il software File protector, effettuiamo tutte le operazioni presenti nel menu file, cioè la cifra e firma di singoli documenti nei diversi formati (p7m, xls, pdf) e cifra e firma di più documenti contemporaneamente o di una cartella completa.

Carta regionale dei servizi della Lombardia

Per i residenti in Lombardia è anche disponibile un programma scaricabile a partire dall'indirizzo: http://www.crs.regione.lombardia.it.

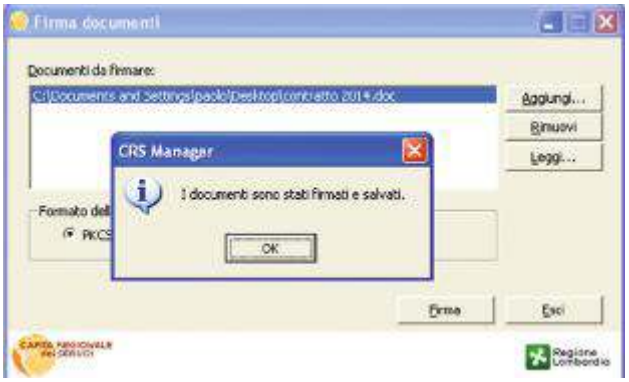
Dopo aver installato il programma, apporre la firma su di un documento è una operazione molto semplice: ▶

Cliccando su firma, è possibile definire il formato di firma desiderato tra pkcs#7 e PDF, quindi si individua il file da firmare: ▶



Per concludere l'operazione di firma viene ora richiesto il PIN: ▶

Dopo qualche secondo si ottiene la conferma che tutto è andato a buon fine: ▶



Nella nostra cartella è ora presente un nuovo file, con estensione p7m, con la seguente icona: ▼

CLIL

Hacker, cracker and lamer

The term hacker hasn't always been the negative title that it is today. A hacker originally described a person with a desire to learn about technology and to experiment and who was technically proficient with whatever systems they hacked. These days, largely due to the popular media, when people hear hacker, they wrongly think criminal. The tech community now distinguishes between hackers, who identify security flaws in order to improve computer systems, and crackers, who attempt to exploit those flaws to their own advantage. Hereafter, we will use the term cracker to refer to computer criminals or people unethically exploiting systems.

Hackers: The White Hats

Just like in the old Hollywood westerns, the good guys wear the white hats, at least metaphorically. White hat is a term often used to describe ethical hackers that stay entirely within the law. They never access a system or network illegally, and they work tirelessly to expose holes in systems with the ultimate goal of fixing flaws and improving security. Upon finding a flaw, a white hat will usually notify the software vendor and give the company a chance to patch the flaw before making the bug public knowledge.

White hats may be security professionals, hired by companies to audit network security or test software. Using the same software tools that crackers use, a white hat seeks to improve the security of his own network by proactively attacking it as a cracker would. White hats may even create software aimed at thwarting tools available to crackers. White hats can use tools such as the Fake AP to thwart wireless sniffers that crackers might use to discover wireless networks.

Knowing how a cracker operates enables a white hat to take steps to secure a network against likely avenues of attack. Although some ex-crackers work as security consultants, simply knowing how to crack a system doesn't translate into being able to secure it. White hats don't acquire their skills illegally. By demonstrating sound judgment and admirable ethics, they make a much better choice for companies looking to hire a security consultant.

Crackers: The Black Hats

Hackers refer to the computer world's outlaws as black hats. The opposite of the white hat, a black hat or cracker breaks into systems illegality for personal gain, vandalism, or bragging rights. A cracker doesn't need to be particularly knowledgeable or skillful; in fact, most of them aren't. Few crackers are skilled enough to create their own software tools, so most rely on automated programs that they download from disreputable Web sites.

Because crackers know they are breaking the law, they do everything they can to cover their tracks. Fortunately, security professionals catch quite a few of them because the majority of crackers lack real skill. When the authorities do catch them, their skill with a computer is often greatly exaggerated to promote the agency making the arrest (and to sell newspapers and commercials).

Still, it's important to acknowledge that crackers present a serious threat: many are technically proficient and can cause a lot of damage, and many systems are so woefully insecure that even technically inept crackers can wreak havoc on them.

Secrecy system

"A secrecy system is defined abstractly as a set of transformations of one space (the set of possible messages) into a second space (the set of possible cryptograms). Each particular transformation of the set corresponds to enciphering with a particular key. The transformations are supposed reversible (non-singular) so that unique deciphering is possible when the key is known." Shannon, C.E., "Communication Theory of Secrecy System".

One-time pad

The one-time pad is the only encryption technique that has been mathematically proven to be uncrackable. While hard to use, it has often been the choice for highly sensitive traffic. Soviet spies used one-time pads in the 1940s and -50s. The Washington-Moscow "hot line" also uses one-time pads. However, the technique is hard to use correctly.

3DES

The DES algorithm has been around for a long time, and the 56-bit version is now easily crackable (in less than a day on fairly modest equipment). An enhancement, and one which is still fairly compatible with DES, is the 3-DES algorithm. It has three phases, and splits the key into two. Overall the key size is typically 112 bits (with a combination of the three keys - of which two of the keys are the same). The algorithm is Encrypt-K3(DecryptK2(EncryptK1(message), where K1 and K3 are typically the same (to keep compatibility).

AES

AES, otherwise known as Rijndael and FIPS-197 is a symmetric block cipher that can accept variable

block length and key length. The specification for AES can use keys with a length of 128, 192, or 256 bits to encrypt blocks with a length of 128, 192 or 256 bits (all nine combinations of key length and block length are possible). Both block length and key length can be extended very easily to multiples of 32 bits. AES can be implemented very efficiently on a wide range of processors in software, or directly in hardware.

Public-Key Cryptography Standards (PKCS)

The Public-Key Cryptography Standards are specifications produced by RSA Laboratories in cooperation with secure systems developers worldwide for the purpose of accelerating the deployment of public-key cryptography. First published in 1991 as a result of meetings with a small group of early adopters of public-key technology, the PKCS documents have become widely referenced and implemented.

PKCS#1: RSA Cryptography
PKCS#3: Diffie-Hellman Key Agreement
PKCS#5: Password Based Cryptography
PKCS#7: Digital Envelope
PKCS#8: Private Key Information Syntax
PKCS#9: Selected Attribute Type108
PKCS#10: Certificate Request
PKCS#11: Cryptographic Token Interface
PKCS#12: Personal Information Exchange Syntax
PKCS#13: Elliptic Curve Cryptography Standard
PKCS#15: Cryptographic Token Information Format

Message digest

A message digest is a cryptographic hash function containing a string of digits created by a one-way hashing formula. Message digests are designed to protect the integrity of a piece of data or media by detecting changes and alterations to any part of a message. They are a type of cryptography utilizing hash values that can warn the copyright owner of any modifications applied to their work.

SHA-3 Selection Announcement

The National Institute of Standards and Technology (NIST) is pleased to announce the selection of KECCAK as the winner of the SHA-3 Cryptographic Hash Algorithm Competition and the new SHA-3 hash algorithm. KECCAK was designed by a team of cryptographers from Belgium and Italy, they are:
Guido Bertoni (Italy) of STMicroelectronics,
Joan Daemen (Belgium) of STMicroelectronics,
Michaël Peeters (Belgium) of NXP Semiconductors, and Gilles Van Assche (Belgium) of STMicroelectronics.

NIST formally announced the SHA-3 competition in 2007 with an open call for the submission of candidate hash algorithms, and received 64 submissions from cryptographers around the world. In an ongoing review process, including two open conferences, the cryptographic community provided an enormous amount of expert feedback, and NIST winnowed the original 64 candidates down to the five finalist candidates – BLAKE, Grøstl, JH, KECCAK and Skein. These finalists were further reviewed in a third public conference in March 2012.

NIST chose KECCAK over the four other excellent finalists for its elegant design, large security margin, good general performance, excellent efficiency in hardware implementations, and for its flexibility.

Certification Authority

A certification authority (CA) is a person entrusted with obtaining unique user identification traits. More often than not certification authorities are employees within organizations for which electronic documents or records, such as bank records, are considered highly sensitive or confidential, and could be used for illicit purposes. These carefully selected employees are granted the authority to authenticate specific individual information regarding potential employees or website visitors. Certification authorities' Internet or work-related computer activities are ultimately audited by way of asymmetric cryptography. (from techopedia.com).

Disk Encryption

Disk encryption is a special case of data at rest protection when the storage media is a sector-addressable device (e.g., a hard disk). Disk encryption methods aim to provide three distinct properties:
the data on the disk should remain confidential;
data retrieval and storage should both be fast operations, no matter where on the disk the data is stored; the encryption method should not waste disk space (i.e., the amount of storage used for encrypted data should not be significantly larger than the size of plaintext).

UNITÀ DI APPRENDIMENTO

4

La sicurezza delle reti

L1 **La sicurezza nei sistemi informativi**
L2 **La sicurezza delle connessioni con SSL/TLS**
L3 **Firewall, Proxy, ACL e DMZ**
L4 **Normativa sulla sicurezza e sulla privacy**

Esercitazioni di laboratorio

1 Intercettare la password di posta elettronica con Sniff'em; 2 Il pacchetto PGP Desktop; 3 Realizziamo una VPN con Packet Tracer; 4 Le Access Control List con Packet Tracer; 5 Certificati digitali con Apache; 6 Realizziamo una VPN P2P con Hamachi

Conoscenze

- Conoscere le problematiche connesse alla sicurezza
- Acquisire le tecniche per la sicurezza a livello di sessione
- Avere individuato i problemi di sicurezza delle email
- Sapere il funzionamento del protocollo SSL/TLS e SET
- Conoscere il concetto di proxy server di DMZ
- Sapere le funzionalità dei firewall
- Conoscere l'evoluzione della giurisprudenza informatica
- Acquisire la normativa relativa alla tutela della privacy e alla sicurezza dei dati

Competenze

- Saper garantire la sicurezza informatica e la riservatezza dei dati personali
- Scegliere e costruire una password forte

Abilità

- Effettuare la valutazione dei rischi
- Utilizzare il software PGP
- Realizzare reti private e reti private virtuali
- Analizzare i protocolli S/MIME e IPsec
- Applicare le Access Control List
- Applicare il concetto di bastion host e DMZ

AREA *digitale*

- Esercizi
- Storia degli attacchi informatici

Soluzioni
Puoi scaricare il file anche da hoepliscuola.it

LEZIONE 1

La sicurezza nei sistemi informativi

In questa lezione impareremo...

- le minacce per le reti
- la valutazione dei rischi per la sicurezza dei sistemi informatici
- la prevenzione e le tecniche per la sicurezza
- i problemi di sicurezza delle mail

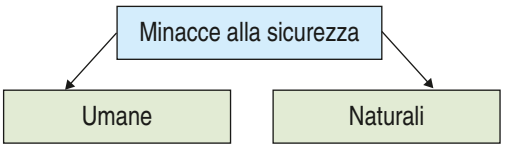
La sicurezza dei dati

La risorsa più importante di ogni organizzazione è l'informazione: grazie all'informazione le aziende operano sui mercati, prendono decisioni tattiche e strategiche, si scambiano dati e documenti; quindi la gestione delle informazioni svolge un ruolo determinante per la sopravvivenza delle organizzazioni. Le informazioni devono essere protette per garantire la ◀ sicurezza informatica ▶.

◀ Per sicurezza informatica si intende l'insieme dei prodotti, dei servizi, delle regole organizzative e dei comportamenti individuali che proteggono i sistemi informatici di un'azienda. Ha il compito di proteggere le risorse da accessi indesiderati, garantire la riservatezza delle informazioni, assicurare il funzionamento e la disponibilità dei servizi a fronte di eventi imprevedibili. ▶

Una prima classificazione sulle possibili situazioni che minacciano l'integrità dei dati individua due tipologie di minacce:

- minacce naturali;
- minacce umane.



Minacce naturali

Le minacce naturali sono dovute a calamità naturali imprevedibili quali tempeste, inondazioni, fulmini, incendi e terremoti che è praticamente impossibile impedire e prevenire.

Per questa tipologia è necessario effettuare una analisi dei rischi in quanto potrebbero causare solo periodi di inattività operativa (danni sulla rete elettrica, fulmini ecc.) dovuti a malfunzionamenti o danneggiamenti delle apparecchiature o delle infrastrutture di comunicazione, oppure danni agli archivi con perdita dei dati.

Oltre al buon senso, che induce ad assumere le misure di prevenzione classiche come il posizionamento dei server in locali protetti, l'utilizzo di sistemi di alimentazione autonoma tramite gruppi di continuità o generatori elettrogeni, il periodico salvataggio dei dati, anche disposizioni legislative (come la legge 196/03) prevedono la messa in atto di misure preventive destinate alle operazioni di disaster recovery, predisponendo dei piani di ripristino e di emergenza.

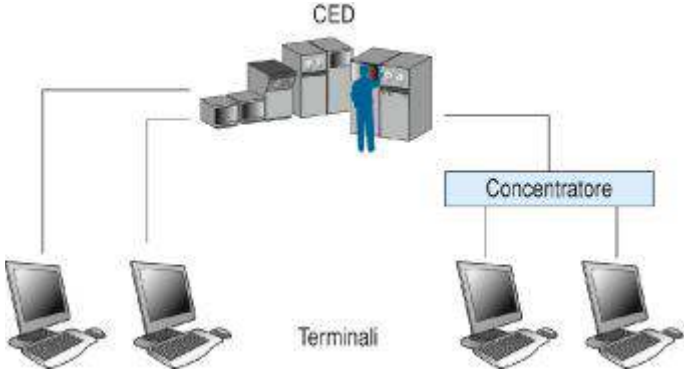
> Tra queste minacce vengono considerati anche gli atti vandalici, le sommosse popolari, le guerre e gli attacchi terroristici che, nonostante siano dovuti a interventi umani, sono di fatto imprevedibili.

Minacce umane

Le minacce umane sono dovute a soggetti che hanno interessi personali ad acquisire le informazioni di una azienda (o di un soggetto) o a limitare l'operatività delle organizzazioni danneggiando i normali processi aziendali. Possono essere causate da personale interno (attacco interno), ad esempio da dipendenti scontenti o malintenzionati oppure da soggetti estranei (attacchi esterni) con lo scopo di creare problemi o danneggiare l'organizzazione.
Le minacce più pericolose sono proprio quelle dovute agli attacchi interni in quanto i dipendenti (o ex dipendenti) conoscono la struttura del sistema informativo e i sistemi di sicurezza che sono in funzione e sono in possesso di autorizzazioni per accedere al sistema (conoscono i codici e le password): questi possono facilmente arrecare danni in quanto, oltre che a carpire informazioni, possono facilmente inserire nei sistemi virus, trojan horse o worm in grado di provocare anomalie di funzionamento in uno o più nodi della rete e trasmettere informazioni del sistema informativo verso l'esterno (es. spyware) oppure creare una testa di ponte verso l'interno (backdoor).
Non sono comunque da sottovalutare anche gli intrusi provenienti dall'esterno che, grazie a programmi come gli "sniffer", intercettano i dati e individuano le password per accedere ai sistemi.

Minacce in rete

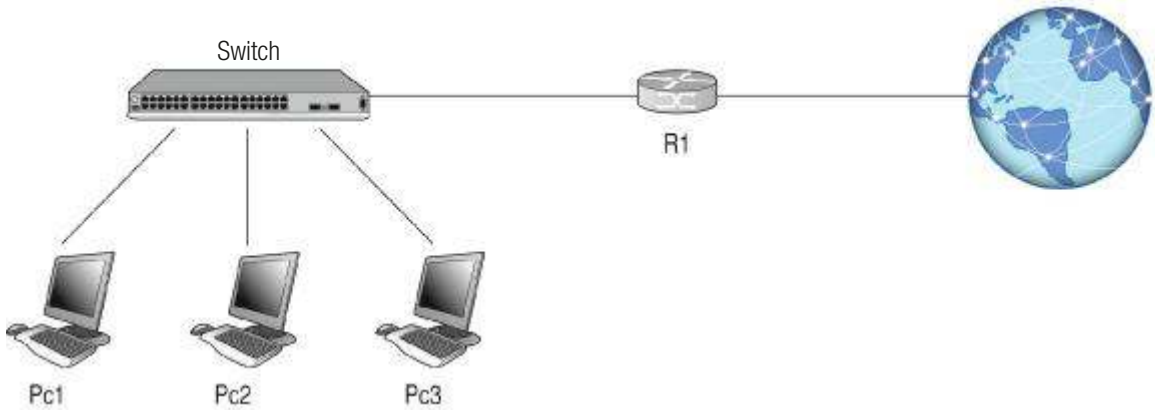
Il problema della sicurezza è "esploso" negli ultimi decenni soprattutto a causa della connettività che ha portato alla modifica dei paradigmi di elaborazione.
Fino agli anni '80 la struttura di un sistema informativo era costituita da un unico elaboratore centrale che conteneva tutte le informazioni e al quale si connettevano postazioni "stupide" che vi accedevano mediante comunicazione "unicast", tramite linee dedicate.



Con le reti locali di personal computer intelligenti e con l'avvento di Internet, le informazioni e l'elaborazione non sono più concentrate ma distribuite e la comunicazione avviene in "broadcast" generalmente su linee condivise.

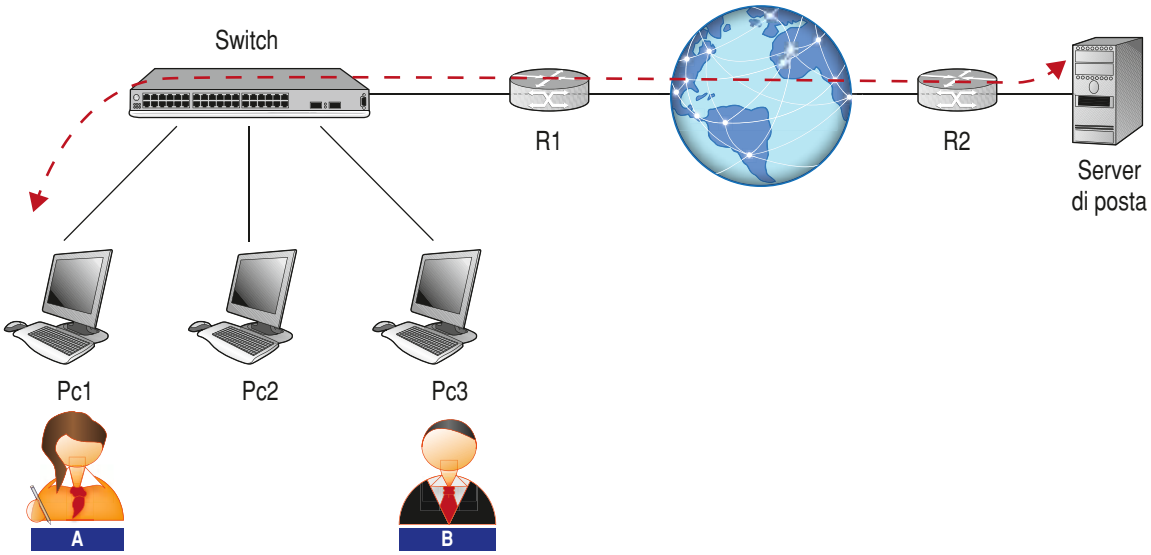
> Le reti locali in "broadcast" costituiscono un punto debole dal punto di vista della sicurezza.

In una rete LAN Ethernet il mezzo fisico di comunicazione (cavo) è condiviso da tutti gli host ed è collassato all'interno dello Switch che ha il compito di amplificare il segnale proveniente da una porta e di ritrasmetterlo sulle altre porte.



La rete aziendale è successivamente connessa a Internet tramite un router in grado di instradare il traffico da e verso l'esterno e quindi è passibile di accessi indesiderati da host esterni aventi lo scopo di compromettere le funzionalità della rete o carpirne informazioni di interesse.

ESEMPIO



Supponiamo ad esempio che l'utente A stia scaricando la propria posta elettronica da un server remoto di posta elettronica e un utente B sia intenzionato a venirne a conoscenza: con un normale ◀ Packet Sniffer ▶ l'utente B può analizzare tutti i pacchetti che circolano su una rete locale, individuare la password dell'utente A, e quindi accedere a sua volta alle informazioni presenti sul server.

◀ I packet sniffer non sono stati realizzati a favore dei cracker ma come programmi di diagnostica delle reti grazie al fatto che sono in grado di catturare, analizzare e decodificare tutti i pacchetti in transito permettendo di individuare gli errori di trasmissione e di conoscere lo stato della rete; di fatto sono divenuti un importante strumento per i malintenzionati. ▶

Sicurezza di un sistema informatico

AREA digitale
Storia degli attacchi informatici

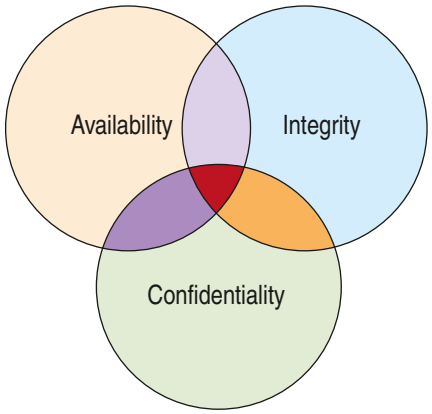
Come ogni sistema di sicurezza l'obiettivo è quello di proteggere e custodire "i propri beni", che nel caso nostro sono le *informazioni* trasmesse, che quindi circolano sulla rete, e i *dati* che sono memorizzati negli archivi.
Il problema della sicurezza nelle reti riveste una grande importanza dato che le reti per loro natura non sono sicure: molteplici sono le minacce e i pericoli per i dati che sono presenti nei diversi host e che circolano sulla rete.

In sintesi, quindi, garantire la sicurezza di un sistema informativo significa impedire a potenziali soggetti attaccanti l'accesso o l'uso non autorizzato di informazioni e risorse.

Con "soggetti attaccanti" intendiamo coloro che cercano di accedere in rete mediante una operazione illegale (attacco informatico) con i più disparati scopi, dalla ricerca di un guadagno economico o politico, alla volontà di danneggiare una organizzazione o una istituzione, alla semplice sfida o divertimento.

I danni che possono derivare dagli attacchi informatici possono essere più o meno gravi a seconda della volontà e del tipo di attacco: possono andare dal furto di danaro o di informazioni, al danneggiamento parziale o totale di archivi o servizi, alla violazione della privacy con la diffusione di dati riservati ecc.

Viene spesso indicata con l'acronimo CIA (dalle iniziali di Confidentiality, Integrity, Availability), dove i primi due termini si riferiscono ai dati mentre il terzo al sistema:
- data confidentiality: mantenere la segretezza dei dati;
- data integrity: evitare che i dati vengano alterati;
- system availability: garantire che il sistema continuerà a operare. ▶



Questi obiettivi sono tra loro strettamente connessi e generano il seguente insieme di aspetti che sono alla base dell'analisi dei rischi della sicurezza di un sistema informativo.
- Autenticazione (*authentication*): con autenticazione si intende il processo di riconoscimento delle credenziali dell'utente in modo da assicurarsi dell'identità di chi invia messaggi o esegue operazioni, evitando che un malintenzionato si spacci per qualcun altro.
  L'identità di un utente può essere verificata per mezzo di conoscenza di informazioni riservate che gli permettono l'accesso al sistema informativo (password), tramite oggetti elettronici (smart card) oppure con strumenti di riconoscimento biologici, quali l'impronta digitale, il fondo retina ecc.
- Autorizzazione (*authorisation*): l'utente autenticato, che quindi può accedere al sistema, deve avere associato *l'insieme delle autorizzazioni*, cioè l'elenco che specifica quali sono le azioni permesse e quali negate, a quali risorse può accedere e quali dati consultare e/o modificare.
- Riservatezza (*privacy*): con riservatezza si intende l'aspetto più classico, cioè che le informazioni siano leggibili e comprensibili solo a chi ne ha i diritti (solo le persone autorizzate): è necessario che gli altri utenti non le possano intercettare o, comunque, non siano in grado di comprenderle.

Nessun utente deve poter ottenere o dedurre dal sistema informazioni che non è autorizzato a conoscere.

- Disponibilità (*availability*): un documento deve essere disponibile in qualunque momento a chi ne è autorizzato; è necessario, quindi, garantire la *continuità* del servizio per ciascun utente che deve poter accedere e utilizzare le risorse e i dati in ogni momento.
- Integrità (*integrity*): con integrità dei documenti si intende l'avere la garanzia e la certezza che un documento sia originale e che il suo contenuto non sia stato letto e/o alterato e modificato da

altre persone non autorizzate: solo chi è autorizzato deve poter portare modifiche ai documenti. È comunque necessario prevenire anche azioni involontarie o maldestre che potrebbero portare al danneggiamento di dati e/o di documenti o di strumenti in grado di verificare se questi eventi sono accaduti.

- Paternità: ogni documento deve essere associato a un utente e questo utente non deve poter ripudiare o negare messaggi da lui spediti o firmati.
  Inoltre spesso è anche richiesto di avere la tracciabilità dei documenti, in modo da sapere chi e quando ha letto o consultato o, semplicemente, ha effettuato un accesso in un archivio.

> Ricordiamo che un documento elettronico ha valenza di prova formale ed è usabile in tribunale, ma deve essere dimostrato in modo innegabile l'autore del documento, cioè l'identificazione e l'autenticazione del mittente e l'integrità del documento.

Le misure da intraprendere per ottenere la segretezza possono essere anche affrontate in diversi livelli della pila protocollare:

- a livello fisico: si può cercare di impedire che avvengano intercettazioni di dati, cioè che intrusi possano connettersi alla rete e prelevare le informazioni;
- a livello di data link: si possono introdurre codifiche e cifrature dei dati trasmessi per renderli incomprensibili ai cracker.

Valutazione dei rischi

Come un qualunque processo aziendale, la valutazione dei rischi può essere studiata scomponendola in fasi e analizzando per ogni fase i singoli componenti che la costituiscono.

Possiamo individuare due fasi essenziali:

1. analisi dei rischi;
2. gestione della problematica.

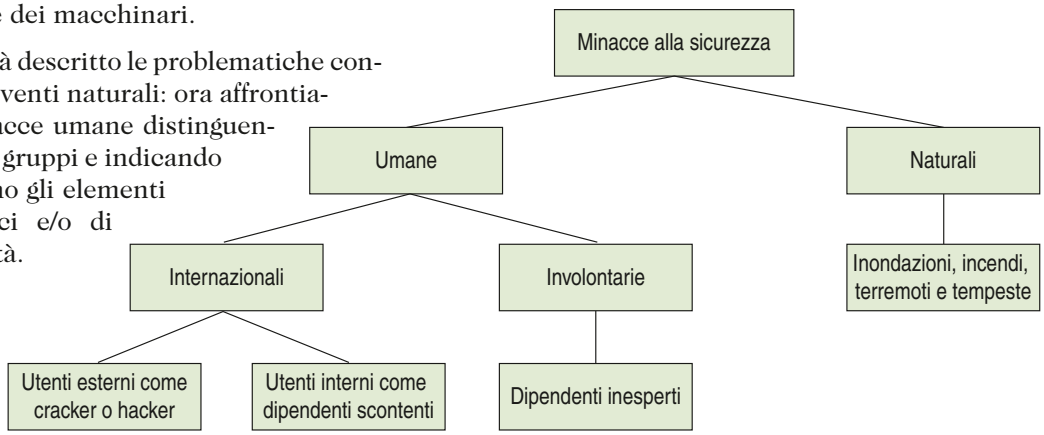
> ◀ Con asset si intende l'insieme di beni, dati e persone necessarie all'erogazione di un servizio IT. ▶

Nella analisi dei rischi si individuano per ogni servizio le situazioni di vulnerabilità dei diversi ◀ asset ▶ e per ciascuna di esse vengono elencate le possibili minacce, dove con minaccia intendiamo un evento intenzionale (attacco) o accidentale che può causare la perdita di una proprietà di sicurezza.

Per ciascun servizio offerto dalla IT gli asset di riferimento dei sistemi informativi sono:

- dati;
- risorse umane;
- risorse tecnologiche;
- locazione dei macchinari.

Abbiamo già descritto le problematiche connesse agli eventi naturali: ora affrontiamo le minacce umane distinguendole in due gruppi e indicando per ciascuno gli elementi caratteristici e/o di vulnerabilità.

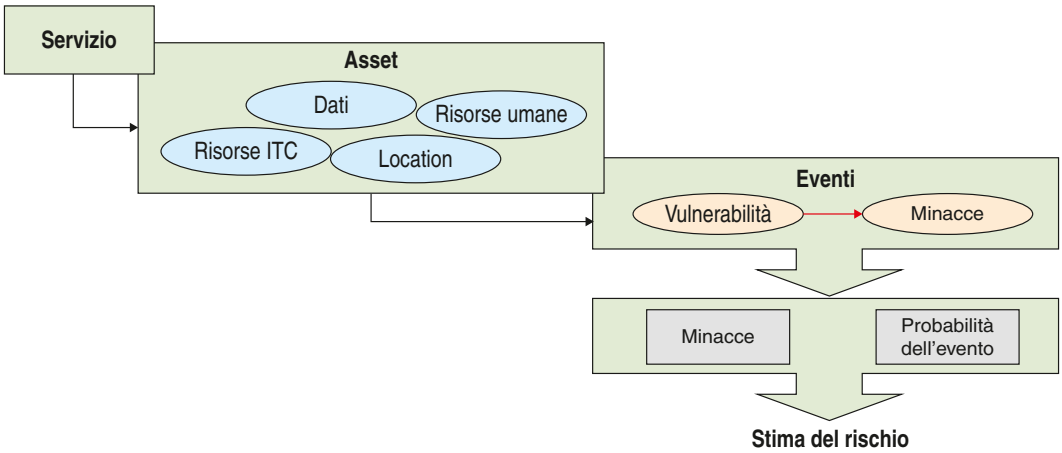


ESEMPIO

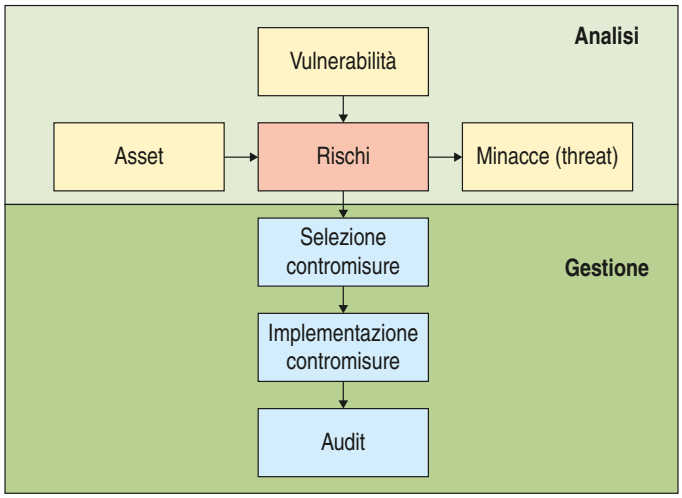
Tra gli eventi intenzionali, cioè gli attacchi, possiamo individuare:
- IP spoofing / shadow server: qualcuno si sostituisce a un host;
- packet sniffing: si leggono password di accesso e/o dati riservati;
- connection hijacking / data spoofing: si inseriscono / modificano i dati durante il loro transito in rete;
- denial-of-service (DoS) e distributed DoS (DDoS): si impedisce il funzionamento di un servizio.

Tra gli eventi accidentali, cioè gli errori e/o malfunzionamenti, possiamo individuare:
- non adeguatezza delle strumentazioni, delle politiche e delle tecnologie di backup;
- locale server sensibile alle inondazioni;
- armadi contenenti i supporti magnetici/ottici non ignifughi;
- errata gestione delle password;
- mancanza di gruppi di continuità;
- ecc.

Per ciascuna situazione di rischio si procede con una stima probabilistica della verificabilità dell'evento dannoso e il grado di dannosità di ciascun evento.



Per ogni evento dannoso si individuano e studiano le possibili contromisure evidenziando quelle che offrono il miglior rapporto prezzo/prestazioni, che siano necessarie e siano effettivamente implementabili. La figura seguente riporta uno schema riassuntivo del *processo della stima dei rischi*.



Si procede con l'implementazione delle contromisure individuate, che necessariamente devono essere seguite da test e valutazioni per analizzarne l'efficacia e l'efficienza.

Principali tipologie di minacce

Per studiare le possibili contromisure da opporre a ogni evento dannoso è necessario in primo luogo individuare e classificare i possibili attacchi ai quali può essere sottoposto un sistema informatico.

Gli aggressori hanno generalmente delle *ragioni* o degli *obiettivi* che vanno dal semplice ostruzionismo che mira a ostacolare le normali attività dell'azienda alla volontà di sottrarre informazioni: per raggiungere questi scopi, utilizzano *tecniche*, *metodi* e strumenti appositi che sfruttano *vulnerabilità* presenti nel sistema, nei controlli o nei criteri di sicurezza.

Obiettivo + Metodo + Vulnerabilità = Attacco

Una prima distinzione tra gli attacchi può essere fatta in attacchi passivi e attacchi attivi che a loro volta hanno diverse possibilità.

Attacchi passivi

- Lettura del contenuto ad esempio mediante lo sniffing di pacchetti sulla LAN;
- analisi del sistema e del traffico di rete, senza analizzare i contenuti.

Attacchi attivi

- Intercettazione: a differenza di quella passiva che si limita a "spiare" i dati (packet sniffing), quella attiva mira a intercettare le password per avere accesso al sistema ed effettuare modifiche ai dati. È possibile che per effettuare l'intercettazione sia necessario un attacco preventivo per istallare componenti hardware (dispositivi pirata) o software specifici. Ad esempio, potrebbero essere inseriti nella rete dei server pirata (shadow server) che si spacciano per i server originali nei quali sono state modificate le tabelle di routing (spoofing) oppure possono essere installati programmi che emulano servizi del sistema registrando al contempo le informazioni riservate digitate dall'utente: potrebbe essere sostituito il programma di login così che quando un utente si connette gli viene intercettata la password (password cracking).
- Sostituzione di un host: sempre tramite la modifica delle tabelle di indirizzamento dei router (IP spoofing) qualcuno si sostituisce a un host falsificando l'indirizzo di rete del mittente (solitamente si falsifica l'indirizzo di livello 3 (IP) ma nulla vieta di falsificare anche quello di livello 2). Questo tipo di attacco prende il nome di source address spoofing e ha lo scopo di effettuare la falsificazione di dati mediante l'accesso non autorizzato ai sistemi informativi.
- Produzione: i malintenzionati producono nuovi componenti che vengono inseriti nel sistema con lo scopo di produrre un danno, e non di prelevare informazioni. Sono dei veri e propri atti di sabotaggio che hanno l'obiettivo di ridurre l'integrità e la disponibilità delle risorse del sistema.
  Le principali tecniche di disturbo sono le seguenti:
  - attacchi virus: programma che provoca danni e si replica "infettando" altri host;
  - attacchi tramite worm: la sua caratteristica è proprio che si replica senza bisogno di "attaccarsi" a un altro programma provocando danni proprio perché "consuma" risorse;
  - attacchi di disturbo denial of service (DoS): in questa categoria rientrano le tecniche che mirano a "tenere occupato" un host con operazioni inutili così da impedire che possa offrire i propri servizi alla rete.
    Alcune tecniche di DoS sono le seguenti:
    - saturazione della posta/log;
    - ping flooding ("guerra dei ping");

  - SYN attack;
  - distributed denial-of-service (DDoS): viene installato un software per DoS su molti nodi costituendo una Botnet: questi programmi sono anche chiamati daemon, zombie o malbot (i daemon sono generalmente controllati remotamente da un master tramite canali cifrati e hanno capacità di auto-aggiornamento).
- Phishing; attraverso spamming di email si attrae un utente su un server pirata (shadow server): in modo da catturare le credenziali di autenticazione o altre informazioni personali; oppure viene invitato l'utente a installare un plugin o una estensione che in realtà sono o virus o trojan. Una variante evoluta è lo spear phishing che include nella mail molti dati personali per aumentare la credibilità del messaggio.
- Intrusione: l'intrusione è l'accesso vero e proprio non autorizzato a uno o più host, che può essere il risultato delle tecniche prima descritte: una volta che un intruso si è introdotto in un sistema può modificare o cancellare le informazioni altrui, prelevare i dati che gli interessano, introdurre dati falsi ecc.

Sicurezza nei sistemi informativi distribuiti

È necessario introdurre delle misure di sicurezza per proteggere sia le informazioni presenti sugli host e circolanti sulla rete, sia le risorse e i servizi che vengono offerti agli utenti rilevando, prevenendo e ponendo rimedio agli effetti di qualunque azione che comprometta la sicurezza stessa delle informazioni.

Effettuiamo una distinzione tra la:
- sicurezza nella rete;
- sicurezza sugli host:
  – a livello di sistema operativo (generale sull'host);
  – a livello di applicazione (solo singolarmente su quei programmi che necessitano protezione).

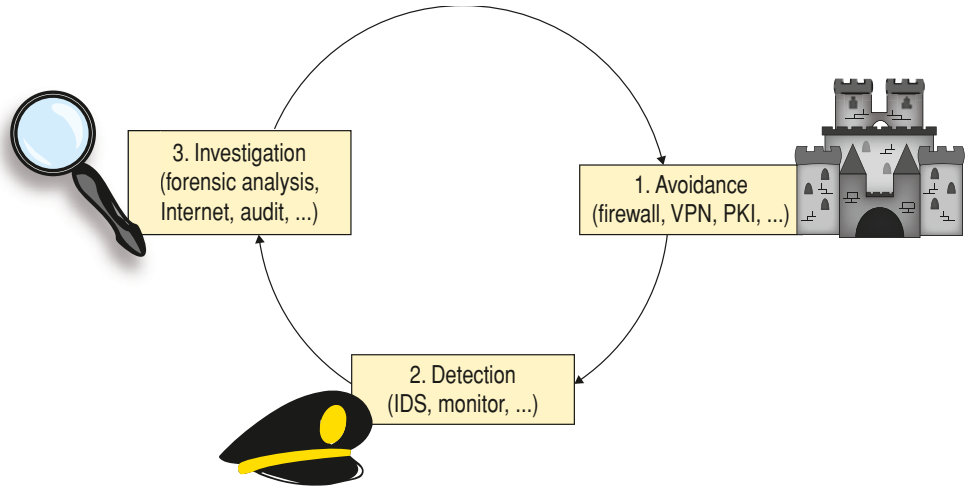
Anche se le problematiche sono tra loro sostanzialmente le stesse e sono tra loro correlate dato che un attacco riuscito su di un host permette al malintenzionato di introdursi anche sulla rete e viceversa: cioè un attacco riuscito alla rete può far scoprire le credenziali degli utenti e permettere di violare gli host che sono a essa connessi.

Scopo di una corretta strategia di sicurezza è proteggere le informazioni importanti e riservate dell'organizzazione, rendendole contemporaneamente disponibili senza difficoltà.
Per sviluppare misure e criteri che consentano di proteggere le risorse e renderle meno vulnerabili, gli amministratori del sistema devono comprendere i diversi aspetti relativi alla sicurezza.

> L'obiettivo di base è quello di garantire al sistema il principio minimo di sicurezza che consiste nella *protezione dagli attacchi passivi* e nel *riconoscimento degli attacchi attivi.*

Per fare ciò si può partire analizzando tutte le componenti del sistema sia fisiche (calcolatori, router, cavi) che logiche (file, processi ecc.) e individuare per ciascuna di esse tutte le tecniche di attacco a essa applicabili, separandole tra attacchi attivi e passivi.
Inoltre è necessario monitorare continuamente la rete in quanto i malintenzionati sono "sempre al lavoro" progettando e realizzando sempre nuove tecniche per sferrare i loro attacchi.

Possiamo quindi riassumere i tre "pilastri" della sicurezza in:
- prevenzione (avoidance) mediante protezione dei sistemi e delle comunicazioni (crittografia, firewall, VPN ecc.);
- rilevazione (detection) mediante il monitoraggio e il controllo degli accessi tramite autenticazione con password e certificati;
- investigazione (investigation) con l'analisi dei dati, il controllo interno con il confronto e la collaborazione degli utenti ecc.



Per quanto riguarda la prevenzione le tecniche adottate sono elencate di seguito e saranno oggetto di apposite lezioni nel seguito della presente unità di apprendimento.

- Uso della crittografia: la crittografia garantisce la riservatezza delle informazioni e l'integrità dei dati trasmessi ed è un efficace prevenzione contro gli attacchi degli sniffer che intercettano i dati in transito sulla rete decodificando i protocolli.
- Autenticazione degli utenti: l'autenticazione garantisce di riconoscere in modo univoco l'identità dell'interlocutore remoto in modo da avere la sicurezza sulla autenticità e la paternità delle informazioni: oltre alla autenticazione con password criptate è possibile implementare meccanismi biologici (impronte digitali, lettura della retina ecc.) per l'autenticazione all'accesso al singolo host in locale e meccanismi di autenticazione che si basano sull'indirizzo IP o MAC dell'host sorgente alla connessione dell'host alla rete.
  Nel dettaglio all'autenticazione dell'utente sono associate tre diverse problematiche:
  – identificazione: risponde alla domanda *"chi sei?"* e consiste nel riconoscimento mediante l'associazione dello user ID alla password o mediante l'uso di smart-card o di dati biometrici;
  – autenticazione: risponde alla domanda *"come mi accerto che sei tu?"*, il cui scopo è quello di verificare l'identità di chi intende utilizzare il sistema e che questa corrisponda a un utente autorizzato;
  – autorizzazione: risponde alla domanda *"cosa posso fare?"*, e in genere è la parte più complessa dei servizi di sicurezza dato che sono molti i modelli di realizzazione che devono integrarsi con le politiche aziendali e le concezioni delle metodologie applicate. Lo schema classico di controllo degli accessi è quello chiamato Discrectionary Access Control o DAC, dove viene definito il proprietario di un dato ed è lui a decidere quale tipo di accesso gli altri utenti possono avere dello stesso.
- Firma elettronica: se firmiamo i documenti con la firma elettronica e abbiamo la garanzie che questa sia autentica e non falsificabile, siamo certi che il documento firmato non è stato alterato e quindi è non ripudiabile in quanto l'autenticazione ne garantisce la paternità.

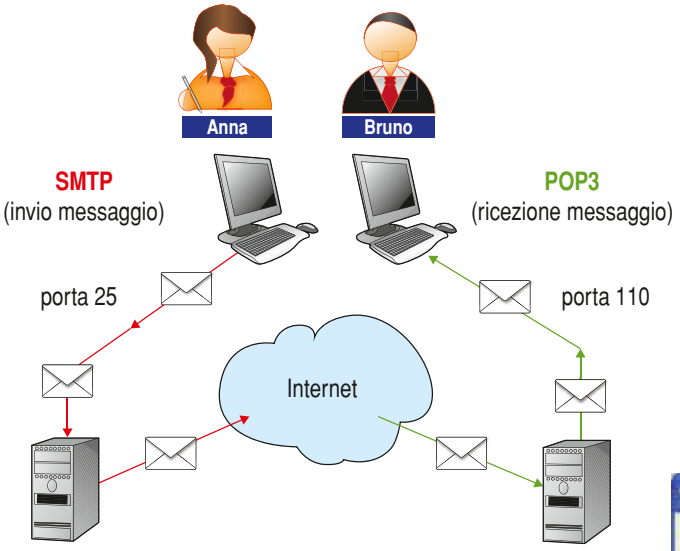
> L'autenticazione delle chiavi pubbliche deve essere effettuata mediante terze parti, le Certification Authority, che garantiscono l'integrità e l'autenticità dell'elenco delle chiavi pubbliche (racc. ITU X.509).

- Connessioni TCP sicure mediante SSL: realizzare delle connessioni sicure a livello di sessione implementando protocolli come il Secure Socket Layer (SSL) che offre i servizi di sicurezza per l'autenticazione delle parti in comunicazione, per garantire l'integrità dei dati e la riservatezza delle comunicazioni.
- Firewall: è un sistema hardware-software dedicato alla difesa perimetrale di una rete che agisce filtrando il traffico di pacchetti entranti e/o uscenti secondo delle regole precedentemente definite;

in fase di configurazione di un firewall, per prima cosa si deve decidere la politica di default per i servizi di rete:
– default deny: tutti servizi non esplicitamente permessi sono negati;
– default allow: tutti i servizi non esplicitamente negati sono permessi.
Generalmente un firewall di rete è costituito da più macchine differenti che lavorano assieme per prevenire accessi non voluti: il router esterno, quello connesso a Internet, invia tutto il traffico entrante all'application gateway che seleziona i pacchetti utilizzando apposite liste di accesso (ACL Access control list) e li inoltra alla rete interna: quindi il gateway filtra il traffico entrante e uscente, eliminando i pacchetti che non soddisfano i requisiti di sicurezza individuati (filtering router).

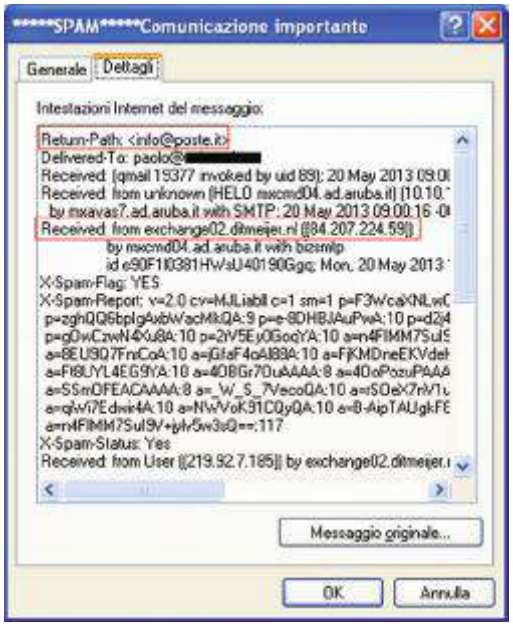
- Reti private e reti private virtuali: è possibile acquistare direttamente presso gli operatori delle reti pubbliche una linea a uso esclusivo della azienda (reti private), ma con costi considerevoli, oppure realizzare una rete privata virtuale VPN creando dei tunnel protetti sulle infrastrutture di Internet mediante connessioni punto-punto di pacchetti autenticati (con contenuto informativo cifrato) incapsulati in pacchetti tradizionali.

La posta elettronica



La posta elettronica è forse il servizio di Internet più importante dato che è utilizzato praticamente da tutti coloro che hanno un account; però, purtroppo, la posta elettronica è pubblica ed è esposta a ogni tipo di attacco informatico.
La posta è lo strumento preferenziale per sferrare attacchi sulla rete dato che il protocollo SMTP non offre alcuna garanzia di riservatezza (il testo viene trasmesso in chiaro): lungo il percorso che intercorre tra il mittente e il destinatario, una email può essere esposta ad attacchi mentre "sosta" in buffer temporanei presso switch, router, gateway e host intermedi nella rete, nonché negli spazi di lavoro dei processi che costruiscono, formattano e presentano il messaggio.

Il fenomeno della contraffazione del mittente della mail, operazione che richiede pochi minuti di "lavoro" e modeste conoscenze di pirateria informatica: generalmente queste mail hanno un allegato, il miglior veicolo per introdurre malware, virus, cavalli di Troia. ▶



In figura si può vedere come questa mail, che già è stata riconosciuta e "marchiata" come SPAM dal server di posta (in questo caso aruba), sia stata inviata da un indirizzo contraffatto (info@poste.it), del quale però possiamo sapere l'indirizzo IP.

Sono possibili due approcci che devono essere combinati assieme, dato che ciascuno riesce solo a proteggere parzialmente dalle minacce possibili:

1. usare una variante sicura del protocollo che garantisca autenticazione e riservatezza (SASL + TLS);
2. spostare la gestione della sicurezza a livello di applicazione e continuare a trasmettere i dati (autenticati e crittati) su un canale insicuro.

Gli obiettivi di una *posta sicura* sono i seguenti:

- integrità: il messaggio non può essere modificato;
- autenticazione: identifica il mittente;
- non ripudio: il mittente non può negare di aver spedito la mail;
- riservatezza: i messaggi non siano leggibili sia in transito sia nella casella postale.

Per ciascuno di questi obiettivi possiamo individuare i possibili attacchi:

- attacco all'integrità:
  - modifica del contenuto del messaggio;
  - falsificazione del contenuto del messaggio da parte di osservatori esterni;
  - falsificazione del contenuto del messaggio da parte del destinatario;
- attacco all'autenticazione:
  - modifica dell'origine del messaggio;
  - falsificazione dell'origine del messaggio da parte di osservatori esterni;
  - falsificazione dell'origine del messaggio da parte del destinatario;
- attacco al non ripudio:
  - negazione della trasmissione del messaggio;
- attacco alla riservatezza:
  - intercettazione e lettura del messaggio;
  - intercettazione e blocco del messaggio;
  - intercettazione del messaggio e successiva ripetizione.

Con la trasmissione di messaggi criptati possiamo risolvere i problemi relativi alla riservatezza e alla falsificazione del messaggio: se inoltre utilizziamo un protocollo dove ogni messaggio contiene qualcosa di univoco che viene crittografato possiamo difenderci anche dalla ripetizione.
Con la crittografia simmetrica non è possibile però difendersi da falsi mittenti, in quanto la chiave pubblica è in comune: inoltre non ci si può proteggere dal blocco della consegna della posta, a meno che il mittente e il destinatario non abbiano concordato spedizioni con protocolli particolari e/o orari/giorni di consegna predeterminati.

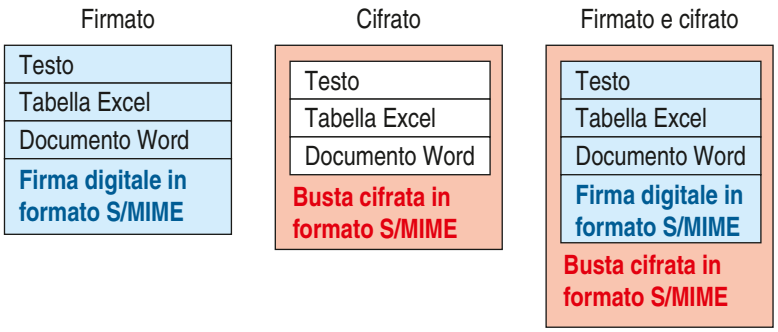
Il protocollo S/MIME per la posta elettronica

Il protocollo SMTP presenta un limite intrinseco dal punto di vista della protezione e una sua possibile alternativa è il protocollo S/MIME che presenta funzionalità avanzate consentendo un'ampia connettività per la posta elettronica senza compromettere la protezione.

S/MIME fornisce due servizi di protezione:

- firme digitali;
- crittografia dei messaggi.

Questi due servizi sono alla base della protezione dei messaggi S/MIME in quanto un messaggio può essere firmato, cifrato oppure essere sottoposto a entrambi i "trattamenti":



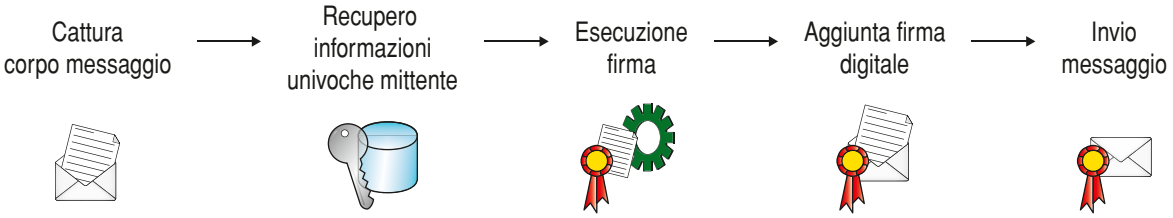
Zoom su...

ALGORITMI DI S/MIME

S/MIME v.3 utilizza i seguenti algoritmi:
- message digest: SHA-1 (preferito) oppure MD5;
- firma digitale: DSS (obbligatorio), digest + RSA;
- scambio chiavi: Diffie-Helmann (obbligatorio) e chiave cifrata con RSA;
- cifratura del messaggio: 3DES con 3 chiavi RC2/40.

Firme digitali

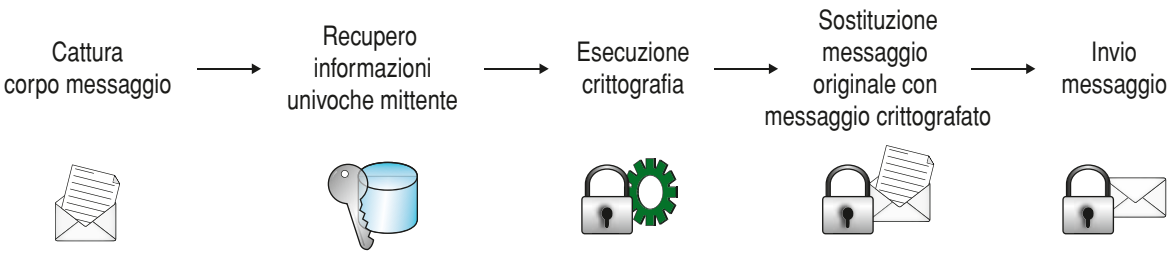
La procedura per apporre la firma digitale da S/MIME è estremamente semplice e si esegue secondo lo schema seguente:



Grazie alla firma digitale vengono garantiti:
- l'autenticazione: cioè la convalida dell'identità, che nella posta elettronica basata su SMTP non è prevista;
- il non ripudio: l'unicità di una firma impedisce al relativo proprietario di disconoscerla;
- l'integrità dei dati: con la firma digitale si ha la sicurezza che il messaggio ricevuto non sia stato modificato durante il trasferimento.

Crittografia dei messaggi

I messaggi di posta elettronica Internet basati su SMTP non sono protetti e possono essere intercettati e letti da qualsiasi utente durante la fase di trasferimento o nell'area stessa in cui sono archiviati: il problema è stato risolto con lo standard S/MIME mediante la crittografia.
Anche per essa la procedura è molto semplice ed è riportata nello schema seguente:



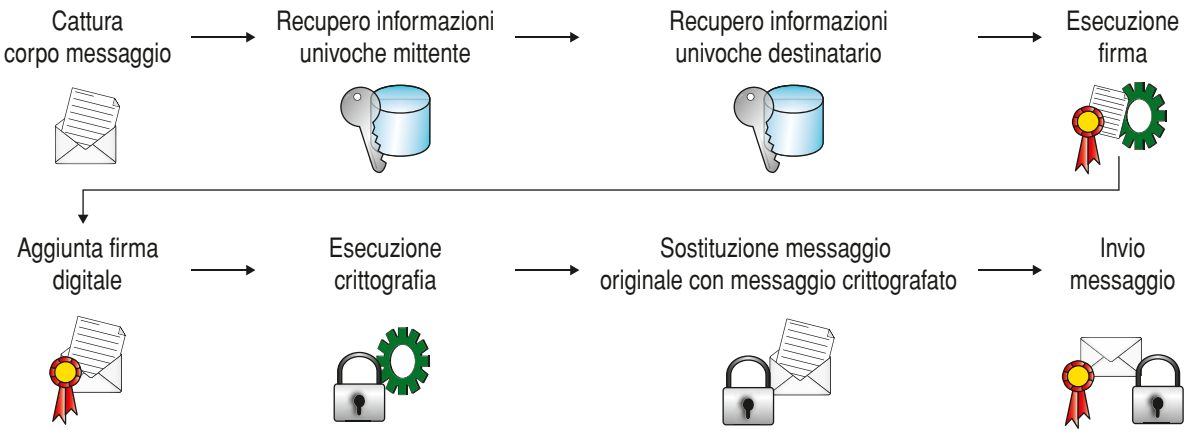
La crittografia ha lo scopo di rendere illeggibile il testo dei messaggi prima che questi vengano inviati attraverso la rete e tramite essa otteniamo due servizi di protezione specifici:
- riservatezza: la crittografia dei messaggi garantisce la riservatezza dei dati ma non esegue l'autenticazione del mittente;
- integrità dei dati: come per la firma digitale, anche la crittografia dei messaggi garantisce l'integrità dei dati.

Interazione delle firme digitali con la crittografia dei messaggi

Per avere tutti i meccanismi di protezione e di sicurezza sulla email è necessario applicare contemporaneamente la firma digitale e la crittografia dei messaggi: la *firma digitale* fornisce il supporto per l'autenticazione e il non ripudio, mentre la *crittografia* garantisce la riservatezza dei messaggi.

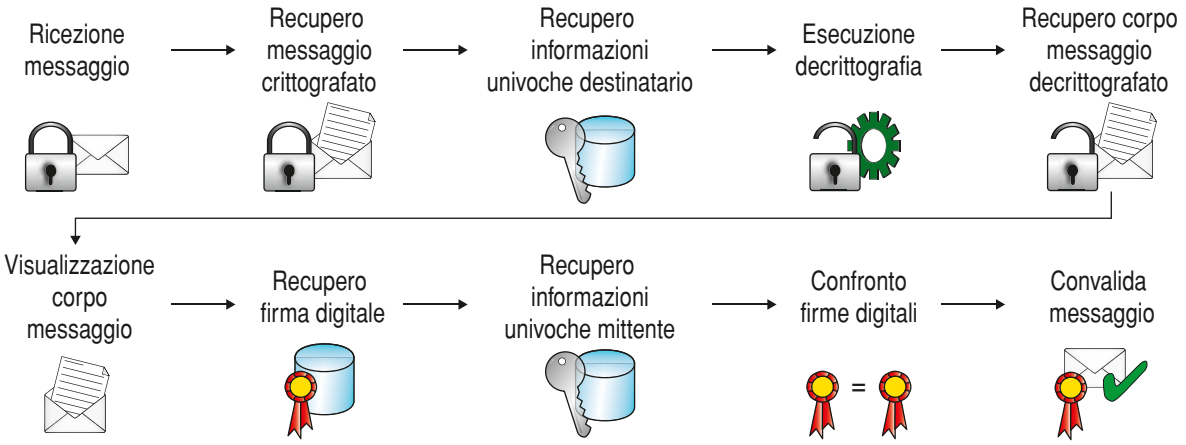
> Con la firma si risolvono le problematiche "relative ai mittenti" del messaggio mentre con la crittografia le problematiche relative alla trasmissione e alla ricezione da "parte dei destinatari".

Vediamo uno schema di applicazione di una firma digitale e quindi della cifratura di un messaggio di posta elettronica che si basa su otto semplici passaggi:



1. acquisizione del messaggio;
2. recupero delle informazioni che identificano il mittente in maniera univoca;
3. recupero delle informazioni che identificano il destinatario in maniera univoca;
4. applicazione al messaggio di una firma generata in base alle informazioni univoche del mittente;
5. aggiunta della firma digitale al messaggio;
6. crittografia del messaggio in base alle informazioni relative al destinatario;
7. sostituzione del messaggio originario con quello crittografato;
8. invio del messaggio.

Analogamente l'operazione di decrittografia del messaggio di posta elettronica e verifica di una firma digitale viene realizzata con 10 semplici passaggi:



1. ricezione del messaggio;
2. recupero del messaggio crittografato;
3. recupero delle informazioni che identificano il destinatario in maniera univoca;
4. decrittografia del messaggio in modo da generare un messaggio non crittografato in base alle informazioni univoche del destinatario;
5. restituzione del messaggio non crittografato;
6. recapito del messaggio non crittografato al destinatario;
7. recupero della firma digitale dal messaggio non crittografato;
8. recupero delle informazioni identificative del mittente;
9. confronto della firma digitale inclusa nel messaggio con quella generata al momento della ricezione;
10. se le firme corrispondono il messaggio è valido.

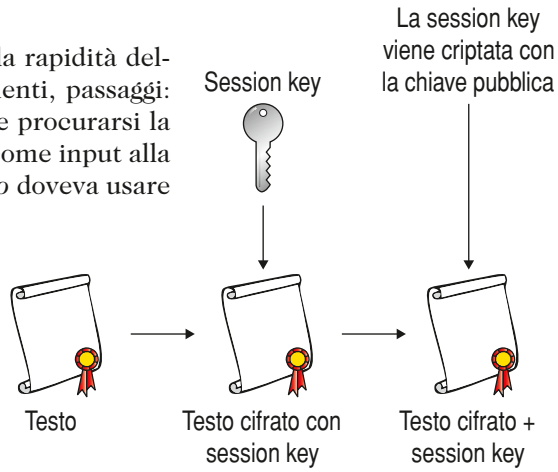
La terza edizione dello standard S/MIME ha ulteriormente migliorato la sicurezza introducendo la tripla crittografia: un messaggio viene firmato, quindi crittografato e infine nuovamente firmato. Questo ulteriore livello di crittografia fornisce una protezione avanzata dei messaggi.

Un software per la posta sicura: PGP

PGP (Pretty Good Privacy) è uno dei più celebri software per la crittografia a chiave pubblica utilizzato soprattutto per codificare le email. Con PGP è infatti possibile crittografare un messaggio e apporre la propria firma digitale, rispondendo in questo modo alle esigenze fondamentali di riservatezza e sicurezza della corrispondenza privata.

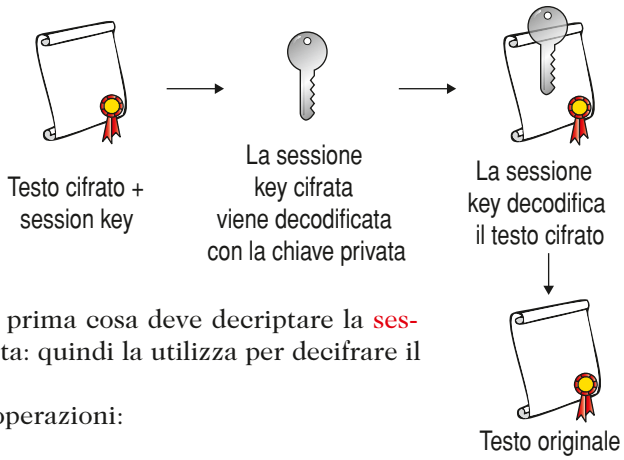
Obiettivo principale di PGP è quello di aumentare la rapidità della codifica RSA, che richiede alcuni semplici, ma lenti, passaggi: *Anna* per inviare un messaggio cifrato a *Bruno* deve procurarsi la chiave pubblica di *Bruno* e immettere il messaggio come input alla funzione unidirezionale del RSA; d'altro canto *Bruno* doveva usare la sua chiave privata e invertire la funzione.

Con PGP per procedere al criptaggio di un messaggio la prima operazione da effettuare è quella di generare una session key: la session key è generata in modo estremamente casuale e verrà usata una sola volta per cifrare il messaggio.
Quindi viene criptata con la chiave pubblica di *Bruno* e inviata assieme al messaggio.



Ma riassumiamo le operazioni che vengono effettuate dal mittente *Anna*:

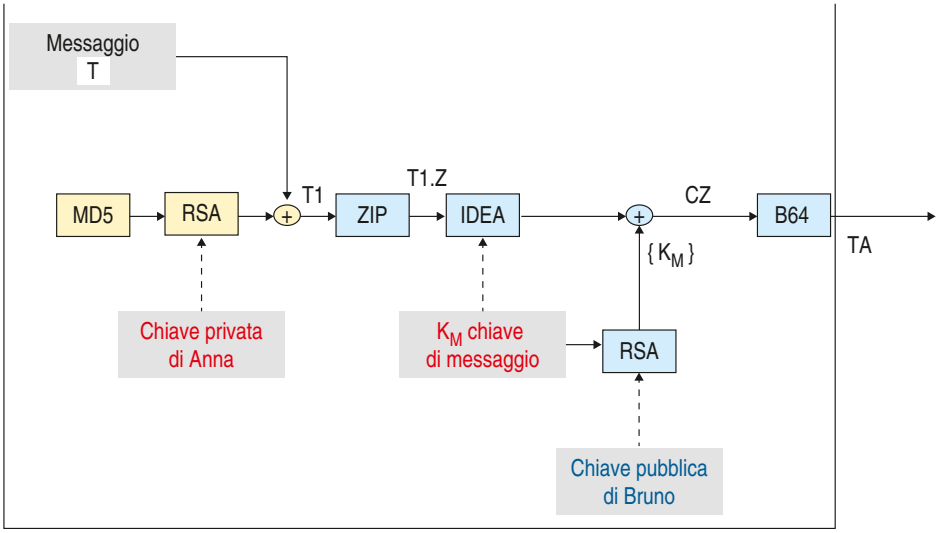
1. *Anna* genera una chiave;
2. si procura la chiave pubblica RSA del destinatario *Bruno*;
3. la utilizza per codificare la chiave simmetrica IDEA;
4. cifra il messaggio attraverso l'uso dell'algoritmo simmetrico IDEA.



Bruno, una volta che riceve il messaggio, per prima cosa deve decriptare la session key e lo fa utilizzando la sua chiave privata: quindi la utilizza per decifrare il messaggio ricevuto.
Bruno dovrà quindi compiere solamente due operazioni:

- *Bruno* usa la sua chiave privata RSA per decifrare la chiave IDEA;
- usa questa chiave IDEA per decifrare il messaggio vero e proprio.

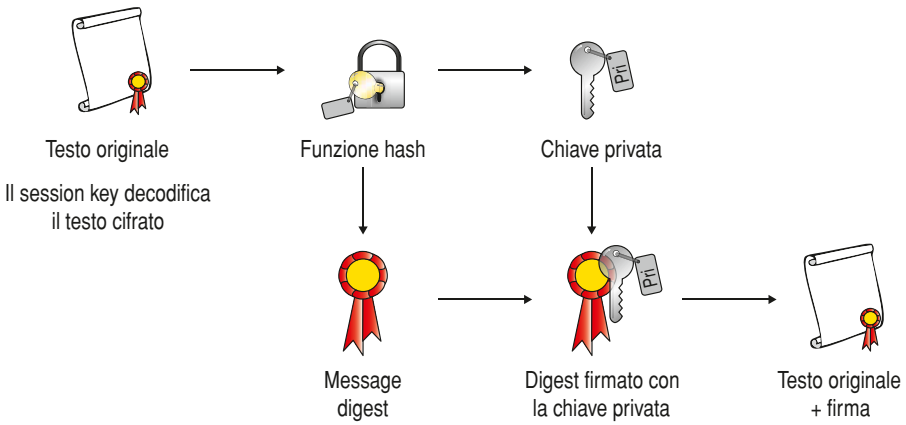
Lo schema completo di funzionamento è il seguente:



T: messaggio di testo in chiaro di *Anna*;
T1: concatenazione di T e della firma hash di T;
T1.Z: T1 compresso;
CZ: concatenazione di T1.Z crittato con IDEA e K_M crittato con chiave pubblica di B;
K_M: chiave monouso del messaggio per IDEA compresso;
TA: Testo ASCII che viene inviato;
Anna si troverà dunque a spedire due informazioni: il messaggio cifrato attraverso l'algoritmo simmetrico IDEA e la chiave simmetrica Km di IDEA cifrata attraverso l'algoritmo asimmetrico RSA.

Firma con message digest

PGP migliora il sistema di firma aggiungendo una funzione "hash unidirezionale" che prende in input il messaggio di lunghezza e genera un output di una lunghezza prefissata, ad esempio 160 bit, che ha la funzione di "checksum", noto come message digest: il digest e la chiave privata sono utilizzati da PGP per creare la "firma", che viene spedita assieme al testo.
Alla ricezione del messaggio PGP ricalcola il digest e lo confronta con quello ricevuto in modo da verificare la correttezza della firma.



La gestione delle chiavi

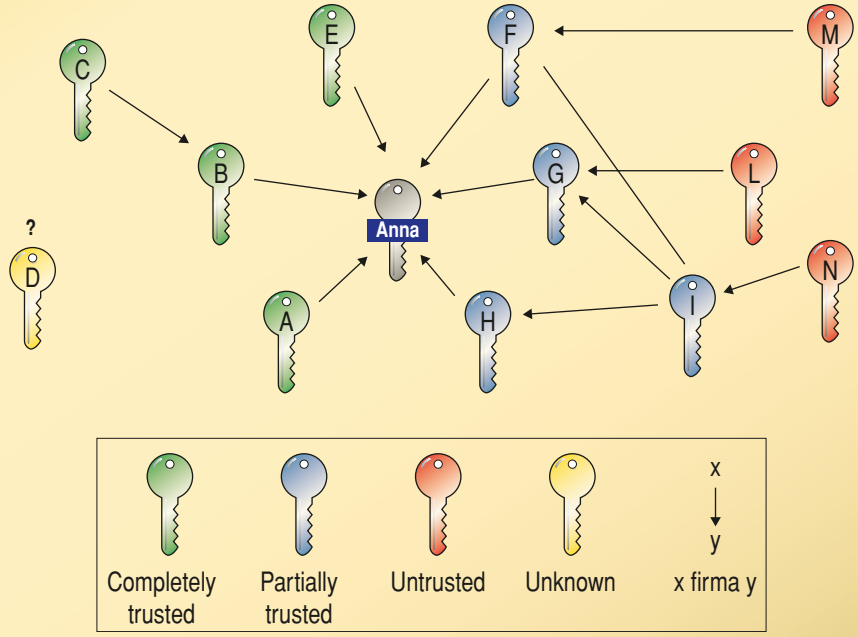
La gestione delle chiavi pubbliche è il fulcro di PGP: è necessario essere certi di cifrare mail con la chiave corretta e non con un falso.
Seguiamo il ciclo di vita delle chiavi:

A vengono generate su base casuale a partire da alcuni input forniti dall'utente: la chiave privata rimane all'utente che la custodisce gelosamente;

B la chiave pubblica deve essere diffusa il più possibile ma deve essere allo stesso tempo certificata, cioè inserita in un certificato in modo che sia garantita la sua autenticità: PGP prevede la possibilità di firmare reciprocamente le proprie chiavi e di creare certificati contenenti la firma di tutti coloro che si fidano del proprietario.

C le chiavi pubbliche sono gestite automaticamente in database accessibili da tutti gli utenti che prendono il nome di keyserver: sono sparsi in tutto il mondo e vengono aggiornati automaticamente in modo da rendere consistente l'insieme di informazioni che gestiscono in modo distribuito e di svolgere anche la funzione di mirroring. Solitamente sono gestiti presso le università, quali ad esempio il MIT negli Stati Uniti e il Dipartimento di Scienze dell'Informazione dell'Università Statale di Milano.
I keyserver possono essere individuati all'indirizzo: http://www-swiss.ai.mit.edu/~bal/pks-commands.html.

È anche possibile individuare diversi livelli di fiducia:
- completely: *del tutto fidato*;
- partially: *parzialmente fidato*;
- untrusted: *non attendibile*;
- unknown: *sconosciuto*.



Verifichiamo le conoscenze

1. Risposta multipla

1 Nella classificazione delle minacce sull'integrità dei dati sono presenti le:

a. minacce naturali
b. minacce accidentali
c. minacce umane
d. minacce terroristiche

2 Indica quale tra le seguenti non è una calamità naturale:

a. tempesta
b. inondazione
c. fulmine
d. incendio
e. alta marea
f. terremoto

3 Indica quale tra le seguenti è classificata come minaccia umana:

a. atti vandalici
b. sommosse popolari
c. guerre
d. spionaggio industriale
e. attacchi terroristici

4 Quale tra i seguenti non rientra tra gli eventi intenzionali?

a. IP spoofing
b. Packet sniffing
c. Connection hijacking
d. Power outage
e. Data spoofing

5 Gli obiettivi di una posta sicura sono i seguenti (indicare quelli non esatti):

a. integrità
b. autenticazione
c. velocità
d. non ripudio
e. allegati cifrati
f. riservatezza

6 Come attacco all'integrità possiamo avere:

a. modifica dell'origine del messaggio
b. modifica del contenuto del messaggio
c. falsificazione del contenuto del messaggio da parte di osservatori esterni
d. falsificazione dell'origine del messaggio da parte di osservatori esterni
e. falsificazione del contenuto del messaggio da parte del destinatario
f. falsificazione dell'origine del messaggio da parte del destinatario

7 Come attacco al non ripudio possiamo avere:

a. intercettazione e lettura del messaggio
b. intercettazione e blocco del messaggio
c. negazione della trasmissione del messaggio
d. intercettazione del messaggio e successiva ripetizione

8 La sigla dell'ente IETF è l'acronimo di:

a. Internet Electric Team Force
b. Internet Engineering Team Force
c. Internet Engineering Task Force
d. Internet Electric Task Force

2. Vero o falso

1 Le minacce naturali non possono essere impedite. V F
2 Non è possibile fare nulla contro le minacce naturali. V F
3 Per le minacce naturali è inutile l'analisi dei rischi in quanto sono imprevedibili. V F
4 Le reti locali in "broadcast" costituiscono un punto debole dal punto di vista della sicurezza. V F
5 I "packet sniffer" sono sviluppati dai cracker per intercettare i pacchetti sulla rete. V F
6 Una minaccia è un evento intenzionale o accidentale che può causare la perdita di sicurezza. V F
7 SMTP non offre alcuna garanzia di riservatezza dato che il testo è trasmesso in chiaro. V F
8 La falsificazione dell'origine del messaggio rientra tra gli attacchi che violano la riservatezza. V F
9 Il protocollo S/MIME presenta funzionalità avanzate rispetto al SMTP. V F
10 PGP è l'acronimo di Private Good Privacy. V F
11 PGP unisce la crittografia asimmetrica RSA e la crittografia simmetrica IDEA. V F

LEZIONE 2

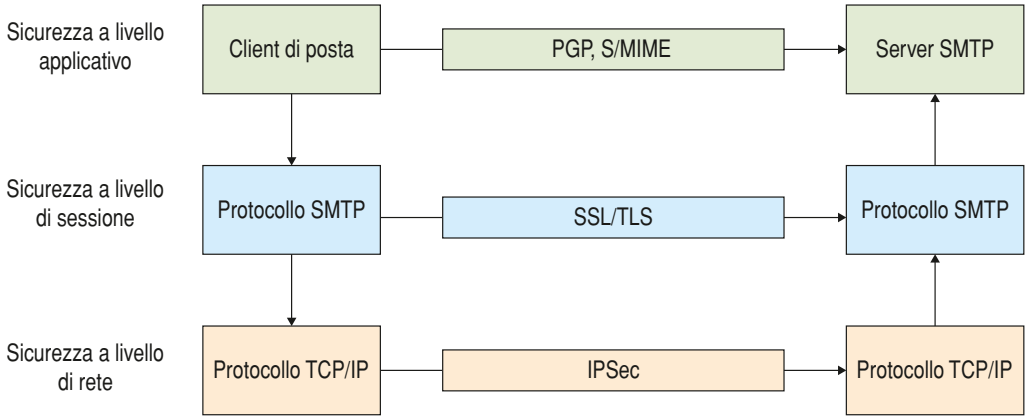
La sicurezza delle connessioni con SSL/TLS

In questa lezione impareremo...

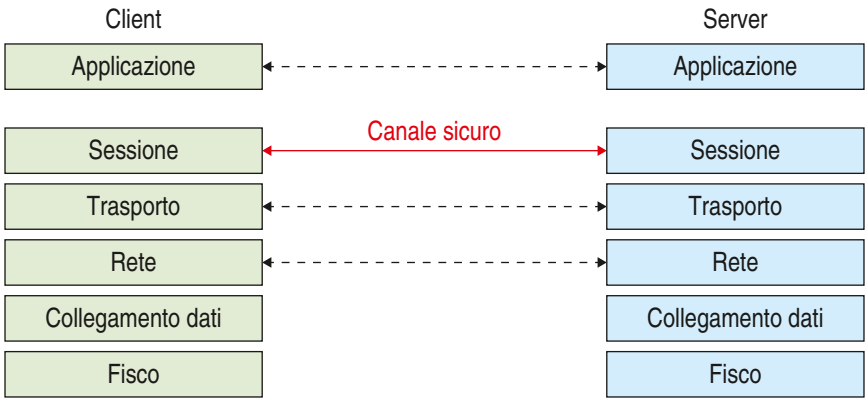
- la sicurezza a livello di sessione
- il funzionamento del protocollo SSL/TLS
- le caratteristiche del protocollo SET

Generalità

I protocolli TCP/IP e SMTP sono per loro natura non sicuri: se per la posta è possibile introdurre meccanismi di sicurezza a livello applicativo (tipo PGP) per tutte le applicazioni Web risulta pressoché impossibile: è stato necessario quindi introdurre dei sistemi di protezione nei livelli inferiori della pila protocollare, a livello di sessione oppure di rete.



Lo standard più diffuso per la protezione dei servizi offerti tramite Internet è Secure Socket Layer (SSL): si tratta di un insieme di protocolli crittografici che aggiungono funzionalità di cifratura e autenticazione a protocolli preesistenti al livello di sessione ed è nato al fine di garantire la privacy delle trasmissioni su Internet permettendo alle applicazioni client/server di comunicare in modo da prevenire le intrusioni, le manomissioni e le falsificazioni dei messaggi.



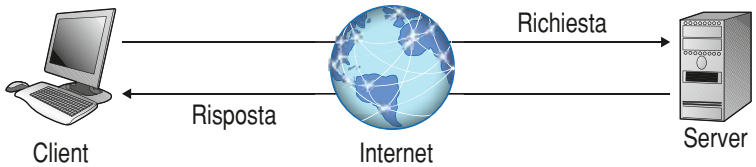
La versione iniziale sviluppata da Netscape è quella comunemente conosciuta come SSL che si è poi evoluta e standardizzata nel protocollo Transport Layer Security (TLS).

Il protocollo SSL/TLS

Il protocollo SSL garantisce la sicurezza del collegamento mediante tre funzionalità fondamentali:

- privatezza del collegamento: la riservatezza del collegamento viene garantita mediante algoritmi di crittografia a chiave simmetrica (ad esempio DES e RC4);
- autenticazione: l'autenticazione dell'identità viene effettuata con la crittografia a chiave pubblica (per esempio RSA e DSS): in questo modo si garantisce ai client di comunicare con il server corretto, introducendo a tale scopo anche meccanismi di certificazione sia del server che del client;
- affidabilità: il livello di trasporto include un controllo sull'integrità del messaggio con un sistema detto MAC (Message Authentication Code) che utilizza funzioni hash sicure come SHA e MD5: avviene la verifica di integrità sui dati spediti in modo da avere la certezza che non siano stati alterati durante la trasmissione.

Tutti i dati trasmessi dal client al server, e viceversa, vengono cifrati.



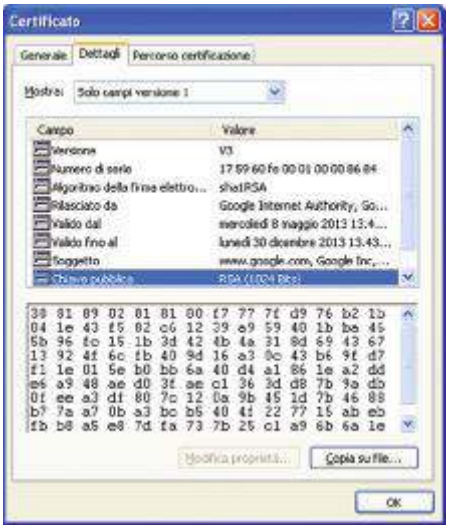
Viene accoppiato molto spesso ad altri protocolli che lavorano a livello applicativo ottenendo meccanismi sicuri come:

- HTTPS (RFC 2818): si ottiene combinando HTTP con SSL/TLS ed è usato per proteggere i dati sensibili inviati da e per i server Web: usa una porta 443 e https:// come prefisso per gli URL;
- S-HTTP (RFC 2660): è poco diffuso e incapsula i dati HTTP in un messaggio crittografato secondo un formato MIME apposito o il formato CMS (Cryptographic Message Syntax);
- SMTPS/POPS/IMAPS: utilizzati per proteggere il contenuto delle email inviate (lavorano sulle porte 465/TCP per SMTPS, 995/TCP per POP3S e 993/ TCP per IMAPS).

HTTPS

Gli indirizzi dei siti protetti con SSL iniziano per https:// e hanno alla loro sinistra l'immagine di un lucchetto: cliccando su di esso viene visualizzata una finestra contenente le autorizzazioni e le caratteristiche della connessione:

Nella prima parte che riguarda l'identità è possibile visualizzare nel dettaglio le informazioni sul certificato (standard X.509 v3) che riportiamo nelle immagini seguenti.



Ogni certificato deve contenere almeno:
- il nome/indirizzo del server, affinché il client possa confrontarlo con il nome della macchina a cui è collegato;
- la chiave pubblica del server;
- il nome dell'autorità certificante.

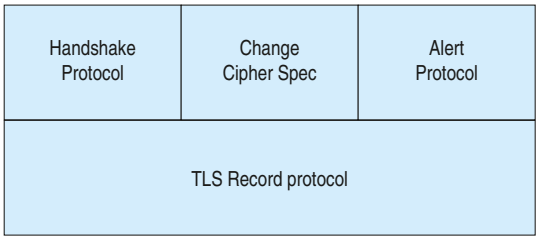
Il certificato è firmato digitalmente dall'autorità certificante che quindi si fa garante dell'autenticità delle informazioni contenute nel certificato. Se l'amministratore di un sito Web decide di utilizzare TLS ha necessariamente bisogno di essere certificato da un CA, generalmente da una root authority, che lo rilascia a pagamento stipulando generalmente contratti annuali (ad esempio VeriSign stipula contratti a partire da $399/anno). È anche possibile generare "in proprio" un certificato, detto self-signed (chi deve essere certificato funge anche da autorità certificante di se stesso), utilizzando ad esempio librerie openssl: parecchi server lo utilizzano per assicurare la riservatezza delle connessioni mediante la cifratura non potendo però garantire l'autenticazione del "proprietario"!

Il funzionamento di TLS

TSL è un protocollo di livello 5 (sessione) che opera quindi al di sopra del livello di trasporto composto da due livelli:
- TLS Record Protocol: opera a livello più basso, direttamente al di sopra di un protocollo di trasporto affidabile come il TCP ed è utilizzato per i protocolli del livello superiore, tra cui l'Handshake Protocol, offrendo in questo modo i servizi di sicurezza;
- TLS Handshake Protocol: si occupa della fase di negoziazione in cui si autentica l'interlocutore e si stabiliscono le chiavi segrete condivise, organizzato in tre sottoprotocolli:
  - handshake protocol;
  - change cipher spec protocol;
  - alert protocol.

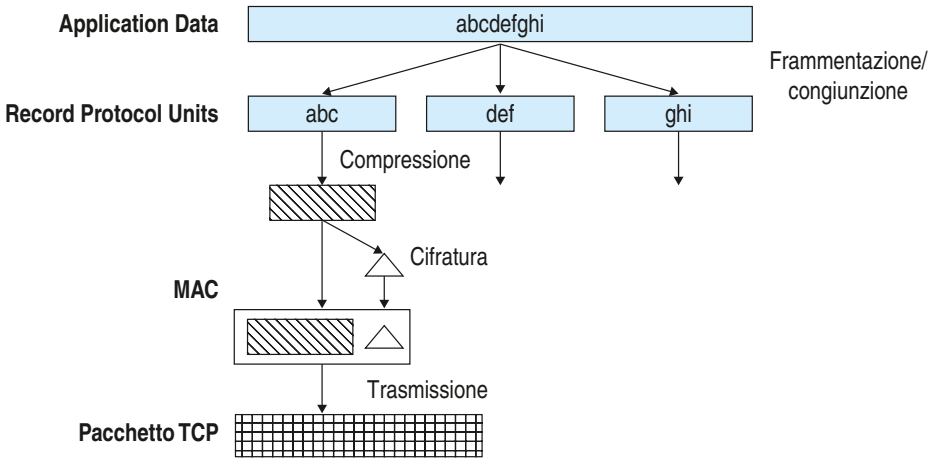
In sintesi, TLS definisce il Record Protocol per trasferire i dati dell'applicazione e stabilisce la sessione utilizzando l'Handshake Protocol.

L'architettura completa di TLS è mostrata a fianco: ▶



TLS Record Protocol

Il TLS Record Protocol prende i dati dal livello superiore, li suddivide in blocchi, eventualmente li comprime, calcola il MAC, cifra il tutto e trasmette il risultato dell'elaborazione.



I dati sono classificati in 4 stati, due correnti e due pendenti: gli stati di lettura (per i record ricevuti) e scrittura (per l'invio dei record) correnti e gli stati di lettura e scrittura pendenti.

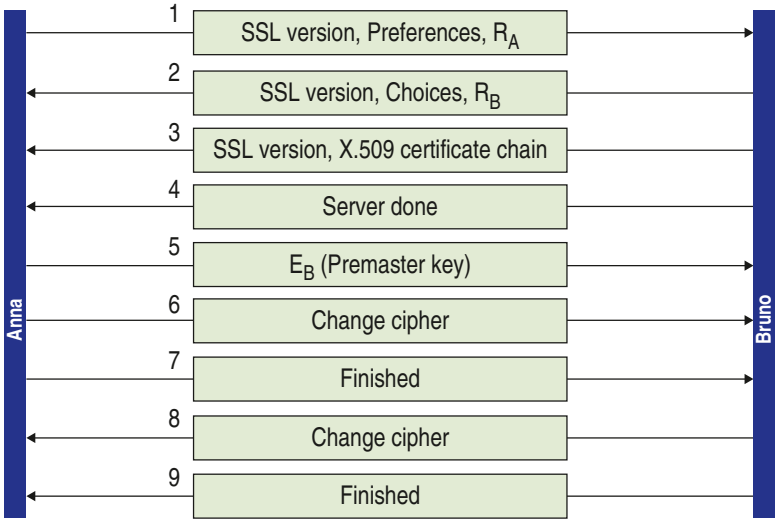
> La differenza tra stato corrente e pendente è in funzione delle operazioni che sono state fatte o meno sui dati stessi: quando sono settati i *parametri* di sicurezza e sono state generate *le chiavi* il dato passa dallo stato pendente allo stato corrente e viceversa.

I parametri di sicurezza sono settati fornendo i seguenti valori:
- *connection end*: specifica se l'entità in questione è il client o il server;
- *bulk encryption algorithm*: indica l'algoritmo di cifratura e i relativi parametri, come la lunghezza della chiave;
- *MAC algorithm*: indica l'algoritmo di autenticazione e i parametri relativi;
- *compression algorithm*: indica l'algoritmo di compressione e i relativi parametri;
- *master secret*: sequenza di 48 byte condivisa tra i due interlocutori;
- *client random*: 32 byte casuali forniti dal client;
- *server random*: 32 byte casuali forniti dal server.

Handshake Protocol

L'Handshake Protocol è responsabile della negoziazione dei parametri di sicurezza di una sessione mediante i suoi tre sotto-protocolli, che permettono inoltre di notificare eventuali situazioni di errore.
La fase di "handshake" vera e propria viene iniziata dal client inviando al server un messaggio di "hello" per iniziare la sessione (1) e proponendo la versione del protocollo e la cipher suite: e il server sceglie il protocol e le opzioni presenti nella suite (2): nel caso non si trovasse l'accordo si procede su livelli inferiori fino a trovare una intesa.
I parametri necessari per la comunicazione sono i seguenti:
- *session identifer:* identificatore della sessione scelto dal server;
- *peer certificate:* certificato X.509 dell'interlocutore (può mancare);
- *compression method*: algoritmo di compressione;
- *cipher spec*: algoritmi di cifratura e autenticazione e relativi parametri crittografici;
- *master secret is resumable*: flag che indica se la sessione può essere utilizzata per iniziare nuove connessioni

Si prosegue con la fase di "change cipher spec": il server invia al client un certificato (3-4) attestante la propria identità e contenente la propria chiave pubblica (ad esempio una chiave RSA): il client ne verifica l'identità, genera una chiave di sessione casuale (premaster key) e la invia al server, cifrandola con la chiave pubblica (5-6-7).
Ora il server decifra il messaggio con la propria chiave privata e ottiene la chiave di sessione che utilizzerà per cifrare/decifrare il successivo traffico dati con un algoritmo simmetrico (ad esempio AES).
Lo schema completo della fase di negoziazione tra *Anna* (client) e *Bruno* (server) è mostrato a fianco: ▶



Conclusioni

SSL permette la cifratura delle comunicazioni tra client e server ma non garantisce l'identità delle parti: nel Web è però fondamentale sapere "con chi si ha a che fare" soprattutto in caso di transazioni con denaro.

La soluzione è stata sviluppata proprio su iniziativa di Visa e Mastercard per l'utilizzo delle carte di credito: si è realizzato il protocollo SET (Secure Electronic Transaction).

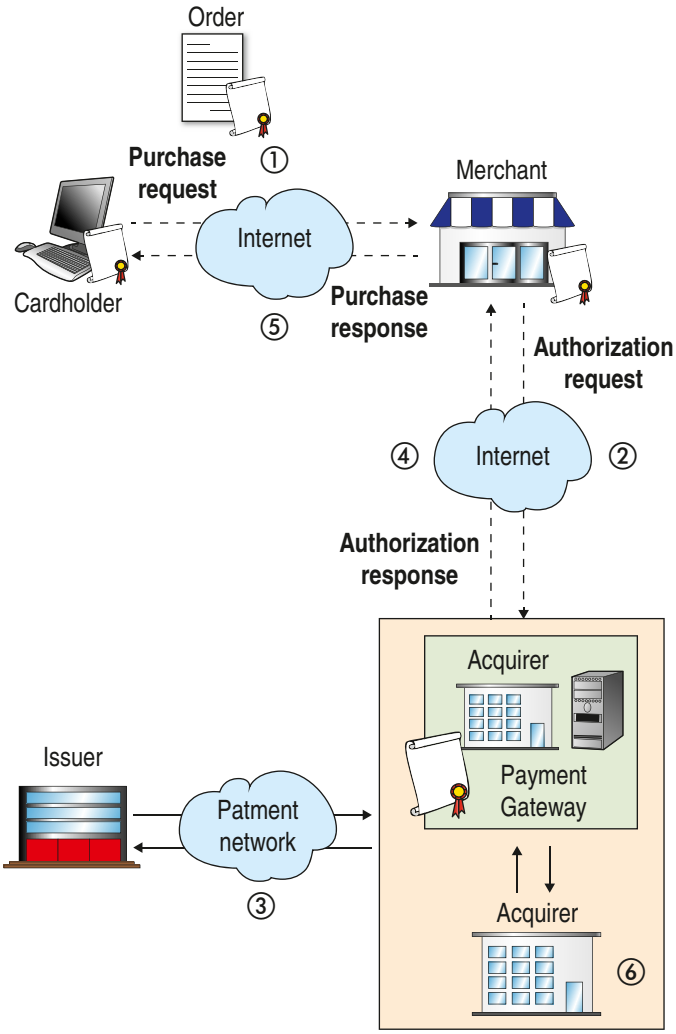
Il SET soddisfa sette importanti requisiti:

1. fornisce confidenzialità nella trasmissione dei dati di pagamento;
2. assicura l'integrità di tutti i dati trasmessi;
3. garantisce che il possessore della carta di credito sia un utente legittimo;
4. garantisce che il commerciante possa accettare le transazioni attraverso il contatto con una istituzione finanziaria;
5. assicura l'utilizzo delle migliori pratiche e tecnologie di sicurezza per proteggere ogni legittima parte coinvolta nella transazione di commercio elettronico;
6. crea un protocollo che non dipende dai meccanismi di trasmissione dei dati;
7. facilita e incoraggia l'interoperabilità fra software e network provider.

Entrano in gioco nuovi attori, tutti muniti di appositi certificati:

- possessore della carta di credito (cardholder): è il cliente che con la sua carta di pagamento interagisce col commerciante tramite il personal computer;
- distributore (issuer): istituzione finanziaria che gestisce gli account finanziari per i clienti e distribuisce le carte di credito; deve autorizzare e, quindi, garantire il pagamento;
- commerciante (merchant): colui che offre in vendita beni o servizi e che preventivamente deve aver concordato ed essere accreditato per riceve pagamenti elettronici da un acquirer;
- acquisitore (acquirer): è l'istituzione finanziaria che gestisce l'account del commerciante e processa le autorizzazioni di pagamento e i pagamenti concreti;
- gateway di pagamento (payment gateway): componente fisica che processa le istruzioni di pagamento sia del commerciante che del cliente; è controllato dall'acquirer o da una designata terza parte.

Seguiamo il flusso delle informazioni dopo che viene effettuato un pagamento mediante SET, come rappresentato nel disegno a fianco. ▶



1. Il possessore della carta di pagamento (cardholder) invia una richiesta di acquisto al venditore merchant contenente le informazioni sulla merce e sul proprio account.
2. Il venditore contatta il gateway di pagamento e chiede l'autorizzazione al pagamento.
3. Il gateway di pagamento verifica l'autenticità della firma del possessore della carta contattando il distributore del possessore della carta (issuer).
4. Se tutto è corretto il gateway invia una risposta di autorizzazione al venditore.
5. Il venditore consegna la merce al possessore della carta.
6. Dopo aver soddisfatto le richieste del possessore della carta di pagamento, il venditore può richiedere l'accredito, presso il suo acquisitore (acquirer), della somma stabilita.

> Le coordinate della carta di credito sono prima codificate con la chiave pubblica dell'issuer poi affiancate ai codici della merce: il numero della carta di credito è fornito in modo crittato e quindi il negoziante non vede il numero in chiaro.

L'unico problema nasce se la carta di credito viene rubata, ma in questo caso il proprietario avvisa subito il proprio issuer che toglie validità al certificato inibendone la validità.

Verifichiamo le conoscenze

1. Risposta multipla

1 Il protocollo SSL garantisce la sicurezza del collegamento mediante le funzionalità fondamentali:

a. privatezza del collegamento
b. autenticazione
c. compressione
d. affidabilità

2 Ogni certificato HTTPS deve contenere almeno:

a. il nome/indirizzo del server
b. la chiave pubblica del server
c. il nome/indirizzo del client
d. il nome dell'autorità certificante

3 TSL è un protocollo di livello 5 composto da due livelli:

a. TLS Record Protocol
b. TLS Alert Protocol
c. TLS Handshake Protocol
d. TLS Change Cipher Protocol

4 Quale tra i seguenti non è un parametro di sicurezza settato nel TLS?

a. Connection end
b. Bulk encryption algorithm
c. MAC algorithm
d. Compression algorithm
e. Peer certificate
f. Master secret
g. Client random
h. Server random

5 Quale tra i seguenti non è un parametro necessario per la comunicazione nel TLS?

a. Session identifer
b. Peer certificate
c. Bulk encryption algorithm
d. Compression method
e. Cipher spec
f. Master secret is resumable

6 SET è l'acronimo di:

a. Secure Encrytp Transaction
b. Secure Electronic Transport
c. Secure Electronic Transaction
d. Secure Encrypt Transport

2. Vero o falso

1 Il Secure Socket Layer (SSL) è un protocollo crittografico a livello di rete. V F
2 SSL è l'evoluzione del protocollo Transport Layer Security (TLS). V F
3 HTTPS si ottiene combinando HTTP con SSL/TLS e utilizza la porta 404. V F
4 Un certificato self-signed viene emesso a pagamento. V F
5 TSL è un protocollo di livello 5 che opera al di sopra del livello di trasporto. V F
6 Nel TLS sono presenti due stati correnti per la lettura e due pendenti per la scrittura. V F
7 SSL permette la cifratura delle comunicazioni e garantisce l'identità delle parti. V F
8 Il protocollo SET è stato realizzato su iniziativa di Visa e Mastercard. V F

LEZIONE 3

Firewall, Proxy, ACL e DMZ

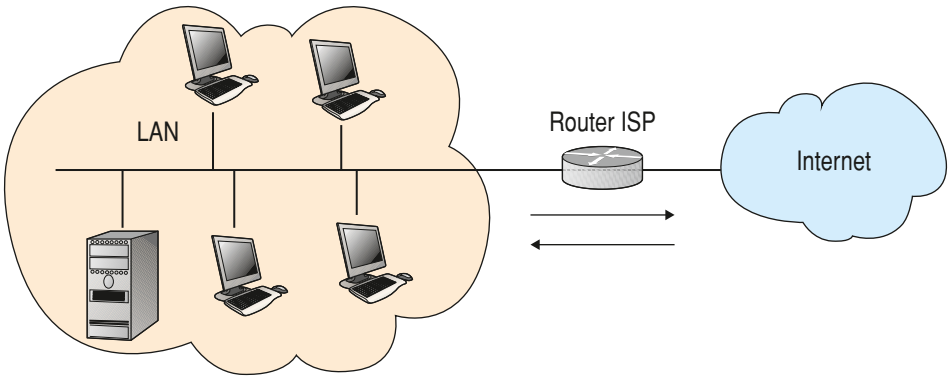
In questa lezione impareremo...

- le funzionalità dei firewall
- le tecniche di filtraggio e le ACL
- il concetto di proxy server di DMZ
- la zona demilitarizzata (DMZ)

I firewall

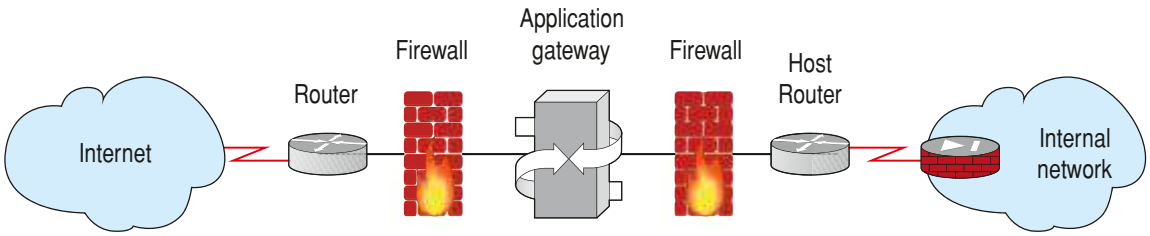
Collegando un router tra una LAN e Internet il traffico viene instradato sia verso l'esterno ma anche verso l'interno della rete, esponendola a rischi di vario tipo derivanti da:

- accessi indesiderati da host esterni aventi lo scopo di acquisire i dati dagli archivi o compromettere i servizi che questa offre;
- installazione di software in grado di provocare anomalie di funzionamento in uno o più nodi della rete oppure di trasmettere informazioni verso l'esterno o semplicemente creare delle porte per poter accedere successivamente nella LAN.



È necessario interporre tra la LAN e il mondo esterno un meccanismo che consenta di controllare "il traffico in transito" e, tramite regole appositamente configurate, di inibire e/o permettere l'accesso agli indesiderati. A questo componente è stato dato il nome di firewall, in analogia con il muro tagliafuoco utilizzato in edilizia che impedisce il propagarsi di un incendio.

Un esempio di organizzazione con firewall è la seguente:



Nel caso di un attacco a una LAN la zona più esposta è quella intermedia e l'attaccante deve superare le difese successive del firewall che regola e limita il traffico tra i server front-end e back-end che comunicano tra loro solo su porte TCP o UDP strettamente necessarie e ben controllate.

Un firewall è un sistema hardware-software dedicato alla difesa perimetrale di una rete che agisce filtrando il traffico di pacchetti entranti e/o uscenti secondo delle regole precedentemente definite. Generalmente un firewall di rete è costituito da più macchine differenti che lavorano assieme per prevenire accessi non voluti: il router esterno, quello connesso a Internet, invia tutto il traffico entrante all'application gateway che seleziona i pacchetti utilizzando apposite liste di accesso (ACL Access control list) e li inoltra alla rete interna: quindi il gateway filtra il traffico entrante e uscente, eliminando i pacchetti che non soddisfano i requisiti di sicurezza individuati (filtering router).

Nella progettazione di un firewall bisogna tenere presente tre principi fondamentali.

1. Il firewall deve essere l'unico punto di contatto della rete interna con quella esterna.
2. Solo il traffico "autorizzato" può attraversare il firewall.
3. Il firewall deve essere un sistema altamente sicuro esso stesso.

Classificazione dei firewall

Una prima differenziazione viene fatta sul tipo di protezione che il firewall deve fare: come già detto, è possibile avere attacchi sia dall'esterno che dall'interno, quindi la prima classificazione riguarda proprio:

- ingress firewall: vengono controllati i collegamenti incoming, gli accessi ai servizi che sono offerti all'esterno della LAN;
- egress firewall: vengono controllati collegamenti outgoing, cioè l'attività del personale interno nella LAN verso l'esterno, in modo da filtrare il traffico in modo che quello non autorizzato o doloso non lasci mai la rete interna.

Il secondo tipo di classificazione prevede il numero di host protetti contemporaneamente:

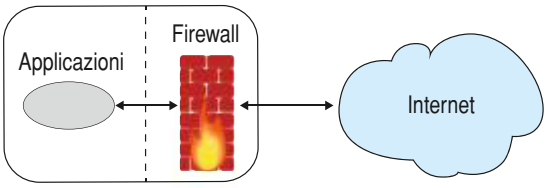
- personal firewall: proteggono il singolo host consentendo, generalmente di default, qualsiasi traffico verso l'esterno (outbound) e bloccando quello dall'esterno (inbound);
- network firewall: si interpone fra la LAN e Internet e controlla tutto il traffico passante.

Un terzo tipo di classificazione viene fatta a seconda del livello di intervento:

- filtri di pacchetto IP: permettono di bloccare o abilitare selettivamente il traffico che attraversa il firewall, definendo i protocolli (o meglio, il tipo di pacchetto), gli indirizzi IP e le porte utilizzate;
- serventi proxy: rappresentano una sorta di intermediario che si occupa di intrattenere le connessioni per conto di qualcun altro nella rete interna.

Personal firewall

Un personal firewall può essere semplicemente un programma installato sul proprio PC che protegge quest'ultimo da attacchi esterni: in essi il traffico dall'interno verso l'esterno è consentito per default mentre il traffico dall'esterno verso l'interno è vietato per default.



I personal firewall sono utilizzabili solo a scopo personale ma impensabili in una azienda in quanto risulterebbero economicamente non convenienti e inoltre sarebbe difficile implementare una politica comune delle policy, dovendo configurare ogni singolo host manualmente.

La sicurezza aziendale inoltre non permette di avere libero il traffico verso l'esterno (pericolo di backdoor, worm ecc.).

I due firewall personali più utilizzati sono quelli inclusi insieme ai sistemi operativi Windows e GNU/Linux: in alternativa si possono scegliere soluzioni di terze parti come ZoneAlarm, Comodo Personal Firewall, BlackICE, Norton Personal Firewall ecc.

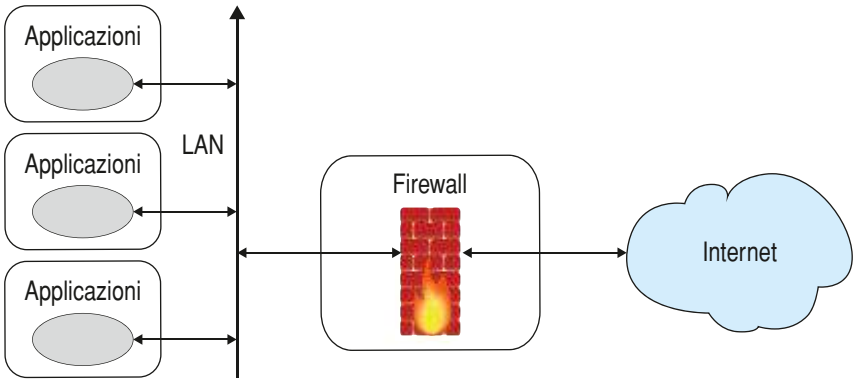
Zoom su...

ZONE ALARM

Zone Alarm è un prodotto completo per la sicurezza che integra perfettamente un pluripremiato antivirus e un firewall che fornisce prestazioni e protezione ottimali. Protegge il PC da virus, spyware, phishing e altri attacchi ed è gratuito per usi domestici: è disponibile per i sistemi operativi più recenti, inclusi Windows 7, Windows Vista, Windows XP, Internet Explorer e Firefox.

Network firewall

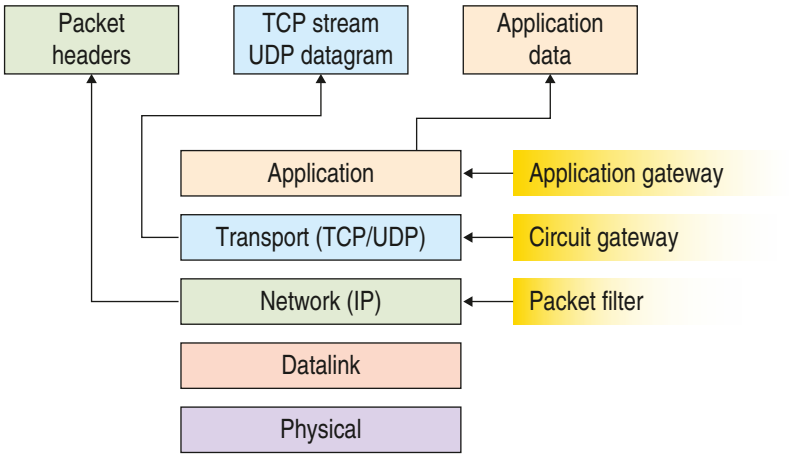
Sono i classici firewall aziendali dove una (o più) macchine sono dedicate al filtraggio di tutto il traffico da e per una rete locale e solo il traffico autorizzato deve attraversare il firewall facendo in modo di mantenere i servizi di rete ritenuti necessari.



A seconda del livello di rete nel quale si fanno i controlli i network firewall possono essere classificati in:

- packet-filtering router: network level gateway;
- circuit gateway: gateway a livello di trasporto;
- proxy server: gateway a livello di applicazione.

Nei sistemi di protezione aziendali spesso sono combinati tra di loro.



Packet filter router

Un packet filtering router scherma i pacchetti dipendentemente dal tipo di protocollo, dall'indirizzo della sorgente e della destinazione e dai campi di controllo presenti nei pacchetti in transito, cioè analizza le informazioni contenute nell'header TCP/IP a livello di rete e di trasporto (packet inspection) per individuare:

- IP del mittente o del destinatario;
- indirizzo MAC sorgente o di destinazione;
- numero di porta verso cui è destinato il pacchetto;
- protocollo da utilizzare.

Il firewall decide se il pacchetto può essere accettato o meno attraverso un algoritmo di scelta che si basa su una lista di regole (in ordine di priorità) precedentemente definite: le filosofie applicabili come regola di funzionamento sono quindi due, diametralmente opposte:

- ciò che NON è specificatamente permesso è proibito (deny);
- ciò che NON è specificatamente proibito è permesso (permit);

e le regole di controllo possono essere configurate in modo statico (manuale) con validità temporale illimitata, oppure dinamico.

Quindi in base a queste regole i pacchetti possono essere:

- accept/allow: il firewall permette al pacchetto di raggiungere la sua destinazione;
- deny: il firewall scarta il pacchetto, senza che questo passi attraverso il firewall e viene inviato un messaggio d'errore all'host sorgente;
- discard/reject: il firewall scarta il pacchetto senza restituire nessun messaggio d'errore all'host sorgente, implementando quella che viene chiamata metodologia *black hole,* che elimina il pacchetto senza che la sua presenza venga rivelata agli estranei.

ESEMPIO

Se si vuole permettere soltanto il traffico sulla porta 80 e 443 le regole di filtraggio dovranno essere del tipo:

Nr. Regola	Azione (Rule)	Host Esterno	Porta	Host Interno	Porta	Descrizione
1	accept	any	any	localhost	80	traffico Web HTTP
2	accept	any	any	localhost	443	traffico Web HTTPS
3	deny	any	any	any	any	default

Fisicamente il firewall viene disposto su un router fra la rete locale e Internet (router di frontiera): dato che devono eseguire molteplici elaborazioni deve disporre di una CPU veloce e di notevole memoria dinamica.

ACL Access Control List

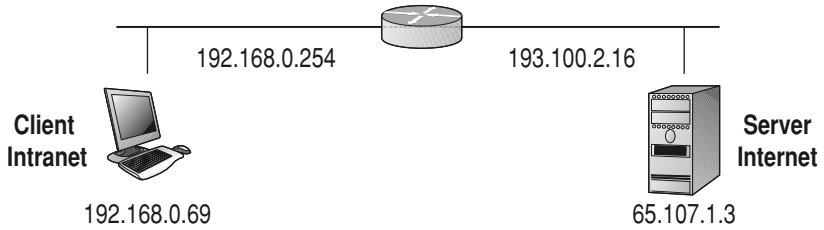
Le regole vengono disposte in liste apposite chiamate ACL (Access Control List) dove è possibile dettagliare i filtri da applicare a ogni pacchetto in funzione delle informazioni presenti negli header TCP/IP, quindi a livello 3 (networking); a volte vengono analizzati anche gli header di livello 4 (transport) ma si ignorano le informazioni del protocollo applicativo al quale il pacchetto si riferisce.

Le ACL si basano o su indirizzo sorgente o destinazione o sui protocolli e sui numeri di porta dei livelli superiori e le filosofie alla loro base sono due, tra loro opposte:

- open security policy: tutto è permesso per default e nella lista ACL è presente l'elenco dei divieti;
- closed security policy: tutto è vietato per default e nella lista ACL sono elencati i pochi accessi che vengono permessi, come nell'esempio precedente, ed è la politica maggiormente adottata.

L'esempio seguente mostra una seconda formulazione di una ACL che consente la connessione di tutti i client di una LAN a un solo indirizzo Web:

Nr. Regola	Azione	Source Address	Source Port	Destination Address	Destination Port
1	allow	any	any /TCP	65.107.1.3	80/TCP
2	allow	65.107.1.3	80/TCP	localhost	any /TCP
3	reject	any	any	any	any



Le ACL possono anche essere inserite su qualunque router anche se trovano la loro applicazione ottimale nei router firewall posizionati tra i router interni e Internet.

Due esempi di ACL frequentemente utilizzati sono:

- Cisco router ACL;
- Linux Netfilter e Iptables.

In questo caso il router ha quindi la funzionalità di NAT e di packet filter.

Configurazione di un router con packet filtering

Configurare un router con packet filtering non è una operazione banale e presenta le seguenti difficoltà:

- in primo luogo è necessario definire le regole sulla base delle quali effettuare le operazioni di filtraggio;
- quindi si deve verificare il corretto funzionamento di queste regole;
- generalmente si è in presenza di protocolli proprietari eterogenei e risulta articolato configurare le funzionalità di packet filtering;
- bisogna individuare ed eliminare le vulnerabilità non documentate, esistenti nelle versioni dei sistemi operativi utilizzati.

Esistono comunque tipi di intrusioni che sono difficili da identificare sfruttando le informazioni base sull'header del pacchetto perché gli attacchi sono indipendenti dal servizio:
- attacchi che falsificano il source address IP (IP Spoofing): tali attacchi possono essere sconfitti scartando semplicemente ciascun pacchetto con un source address IP interno ma proveniente da una delle interfacce del router che sono rivolte verso l'esterno;
- attacchi source routing: possono essere sconfitti semplicemente scartando tutti i pacchetti che contengono source route nel campo option del datagramma IP;
- attacchi con piccoli frammenti: un attacco con piccoli frammenti può essere sconfitto scartando tutti i pacchetti in cui il campo protocol type sia pari a 6 (cioè TCP) and l'IP fragment-offset sia pari a 1.

I principali vantaggi nell'utilizzo di un packet filtering router sono:
- trasparenza: l'utente non si accorge della presenza del firewall dato che non lavora a livello applicativo e quindi non ostacola in alcun modo il normale utilizzo della rete;
- velocità: effettuando minori controlli rispetto agli altri firewall che descriveremo in seguito risulta essere il più veloce e semplice da implementare;
- immediatezza: tramite la definizione di una singola regola si può difendere un'intera rete dai pericoli derivanti da quel tipo di traffico;
- gateway-only: non sono richieste ulteriori configurazioni aggiuntive per i client;
- topologia della rete interna invisibile dall'esterno: se viene aggiunto un NAT, dall'esterno l'unico host visibile è il gateway.

Per contro, gli svantaggi nell'uso di un packet filtering router sono:
- basso livello: un packet filtering router è veloce ma non è in grado di elaborare le informazioni dei livelli superiori a quello di rete e quindi non è in grado di bloccare attacchi mirati a vulnerabilità di una specifica applicazione;
- mancanza di servizi aggiuntivi: non permettono la gestione di servizi quali l'autenticazione, l'HTTP object caching e il filtraggio di URL e dei contenuti delle pagine Web;
- logging limitato: analizzando solo i pochi campi presenti nell'header del pacchetto genera dei file di log con poche informazioni che generalmente sono insufficienti per verificare se il firewall compie sempre il proprio dovere;
- vulnerabile allo spoofing: dato che vengono filtrati i pacchetti in base alla loro provenienza i casi di IP Spoofing non vengono riconosciuti;
- testing complesso: è lungo e complicato effettuare le prove che ne verifichino il funzionamento.

Stateful inspection

I firewall stateful inspection, anche detti *firewall di seconda generazione*, effettuano il filtraggio non sul singolo pacchetto ma sulla connessione (da qui il nome statefull).
Alla richiesta di connessione, se questa viene accettata e quindi non bloccata dalle regole di filtraggio, vengono memorizzate le sue caratteristiche in una tabella di stato in modo che i successivi pacchetti non vengano più analizzati ma, una volta riconosciuti, gli venga permesso il transito, risparmiando al firewall notevoli quantità di elaborazione.

Nella tabella di stato per ogni connessione sono memorizzati i seguenti dati:
- l'identificatore univoco del collegamento di sessione;
- gli indirizzi IP dell'host sorgente e di destinazione;
- le interfacce di rete utilizzate;
- lo stato della connessione, che può essere:
  - handshaking, se si è nella fase iniziale, quella in cui si raccolgono le informazioni e si salvano nella tabella di stato,
  - established, se la connessione è stata stabilita;
  - closing, se la connessione è terminata e si sta per eliminare la entry.

Un esempio di tabella è riportata di seguito:

Source Address	Source Port	Dest. Address	Dest. Address	Connection State
192.168.0.16	1050	192.168.1.33	80	handshaking
192.168.0.100	1250	192.168.1.23	25	established
192.168.0.106	1120	192.168.1.13	443	established
192.168.0.26	1230	192.168.1.03	80	closing

Utilizzando queste informazioni il firewall analizzerà ogni pacchetto per verificare se al computer che sta trasmettendo i dati è consentito effettuare una connessione col computer che deve riceverli.

Al termine della connessione viene eliminata la entry che la descrive dalla tabella, in modo da recuperare spazio: se una applicazione ha periodi di inattività ma è necessario tenerla aperta è sufficiente che di tanto in tanto invii segnali di *keep-alive*.

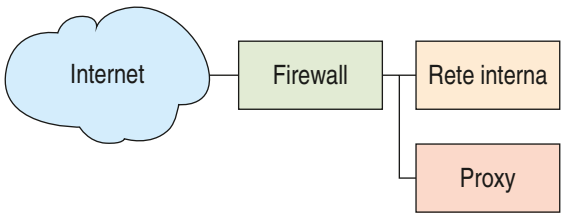
I principali vantaggi nell'utilizzo di uno stateful inspection packet filter router sono:
- buon rapporto prestazioni/sicurezza: offre un ottimo compromesso fra prestazioni e sicurezza dato che effettua meno controlli durante la connessione ed è più affidabile di un filter router;
- protezione da IP spoofing e session hijacking: dato che il controllo viene effettuato sulla connessione è molto più difficile riuscire a violarlo;
- tutti i vantaggi del packet filtering: ha anche tutti gli altri vantaggi dei packet filter dato che ne è una diretta evoluzione (immediatezza, possibilità di natting, gateway-only …).

Per contro, gli svantaggi nell'uso di uno stateful inspection packet filter sono:
- protocollo unico: sfruttando molte delle caratteristiche proprie del protocollo TCP risulta difficilmente utilizzata all'interno di altre infrastrutture di rete;
- servizio di auditing limitato: come per il packet filter le informazioni che registra nei file di log sono ancora insufficienti per una completa diagnostica;
- mancanza di servizi aggiuntivi: lavorando ai livelli inferiori come il packet filter non permette servizi aggiuntivi come la gestione delle autenticazioni e il filtraggio dei contenuti;
- testing complesso: è lungo e complicato effettuare le prove che ne verifichino il funzionamento e la sua corretta configurazione.

Application proxy

Un gateway a livello di applicazione permette di realizzare una politica di sicurezza molto più severa di un semplice packet filtering router: in esso non vengono analizzati e filtrati i pacchetti ma vengono gestite le applicazioni utilizzando un apposito programma detto proxy.

Il proxy è un programma che viene seguito sul gateway che funge da intermediario a livello di applicazione, ad esempio tra il computer dell'utente e Internet; nelle applicazioni client-server un application proxy comunica con il client simulando di essere il server, e viceversa, comunica con il server simulando di essere il client.



Mentre un packet filter è capace di utilizzare soltanto informazioni di basso livello come indirizzi IP e numero di porta, un application proxy è in grado di ispezionare l'intera porzione dati del pacchetto ed è in grado di bloccare pacchetti FTP che contengono certi nomi di file, così da inibire la connessione con determinate pagine o siti Web.

ESEMPIO

Vediamo praticamente come avviene il funzionamento in presenza di un proxy:

- **A** un host della LAN invia al firewall una richiesta di connessione con un sito Web;
- **B** il proxy raccoglie la richiesta, controlla il set di regole per assicurarsi che essa sia lecita, per poi rigenerarla e inviarla al server;
- **C** quest'ultimo riceve la richiesta del proxy come se fosse partita dall'host e invia a esso la risposta;
- **D** risposta che viene nuovamente analizzata dal proxy prima di essere inviata all'host interno.

I principali vantaggi nell'utilizzo di un gateway a livello di applicazione sono:

- controllo completo: dato che utilizza anche le informazioni contenute nel body, effettua un doppio controllo, sia quando viene inviata la richiesta che quando si riceve la risposta;
- log dettagliati: avendo a disposizione anche le informazioni di livello applicativo produce dei file di log molto accurati;
- nessuna connessione diretta: tutti i dati in transito sono analizzati e ricostruiti: tentativi di buffer-overflow o simili sono intercettati e non vengono inoltrati all'host interno;
- sicurezza anche in caso di crash: nel caso di un crash del proxy la LAN risulta isolata e quindi inaccessibile dall'esterno rimanendo protetta;
- supporto per connessioni multiple: è in grado di gestire connessioni separate che appartengono alla stessa applicazione;
- user-friendly: è semplice configurare le regole di filtraggio rispetto a quelle di un packet filtering router;
- autenticazione e filtraggio dei contenuti: offre anche il servizio autenticazione dell'utente e il riconoscimento dei contenuti;
- cache: effettua il caching delle pagine Web e quindi offre un ulteriore servizio liberando la rete da traffico inutile nel caso di richiesta della stessa pagina;

Per contro, gli svantaggi nell'uso di un gateway a livello di applicazione sono:

- è poco trasparente: richiede che ogni computer della LAN interna sia configurato per utilizzare il proxy;
- richiede un proxy per ogni applicazione: è necessario dedicare un proxy a ogni servizio che si ha necessità di far passare attraverso il firewall e, data la dinamicità con la quale vengono offerti servizi in rete, è necessario il suo continuo aggiornamento;
- ha basse performance: la gestione della connessione attraverso il proxy richiede molto lavoro per la CPU e quindi ha prestazioni molto inferiori rispetto ai firewall delle generazioni precedenti.

Bastion host

Con il termine ◀ bastion host ▶ indichiamo l'host configurato per respingere attacchi contro la rete interna e più in generale tutti quegli host che fungono da firewall critici per la sicurezza della rete stessa.

◀ Quando l'application proxy rappresenta l'unico punto di contatto con la rete esterna prende il nome di bastion host, poiché è appositamente corazzato e protetto per resistere agli attacchi. ▶

Nel progetto di una rete nessun host della rete può accedere a Internet senza passare attraverso il bastion host e nessun computer di Internet può accedere alla rete senza passare attraverso il bastion host.

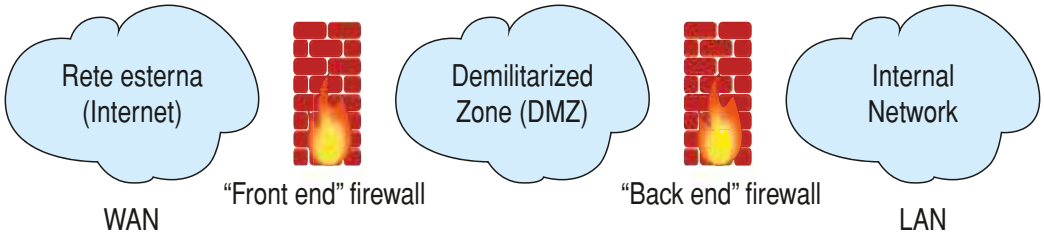
Il bastion host viene sempre associato a un packet filter con politiche di sicurezza opportunamente configurate. Possiede in genere le seguenti caratteristiche:

- unico calcolatore della rete interna raggiungibile da Internet e massicciamente protetto;
- dotato di software strettamente necessario, il più possibile privo di bug utilizzabili come vie di accesso preferenziali;
- proxy server in ambiente isolato (chrooting);
- file system a sola lettura;
- numero minimo dei servizi e nessun account utente;
- salvataggio e controllo dei log;
- eliminazione dei servizi non fidati e disattivazione del source routing.

DMZ

DMZ è la sigla di Demilitarized Zone (zona demilitarizzata) ed è una "sezione di rete" delicata e importante per i processi di sicurezza.
La zona demilitarizzata è una porzione di rete che separa la rete interna dalla rete esterna: i server nella DMZ sono accessibili dalla rete pubblica, perciò non sono trusted (dalla rete interna) e quindi devono essere segregati in quanto, se venissero compromessi, questo non deve produrre effetti collaterali nella rete aziendale.

La DMZ permette di effettuare la sicurezza perimetrale, cioè protegge una rete nei punti in cui essa è a contatto con il mondo esterno, interponendosi tra la LAN aziendale e la WAN esterna:



- il lato LAN (local area network) è il segmento privato e protetto, e a esso appartengono tutti gli host e i server i cui servizi sono riservati all'uso interno;
- la zona WAN (wide area network) è la parte esterna, e a essa appartengono uno o più apparati di routing che sostengono il traffico da e per la rete locale, sia verso Internet che verso eventuali sedi remote dell'azienda.

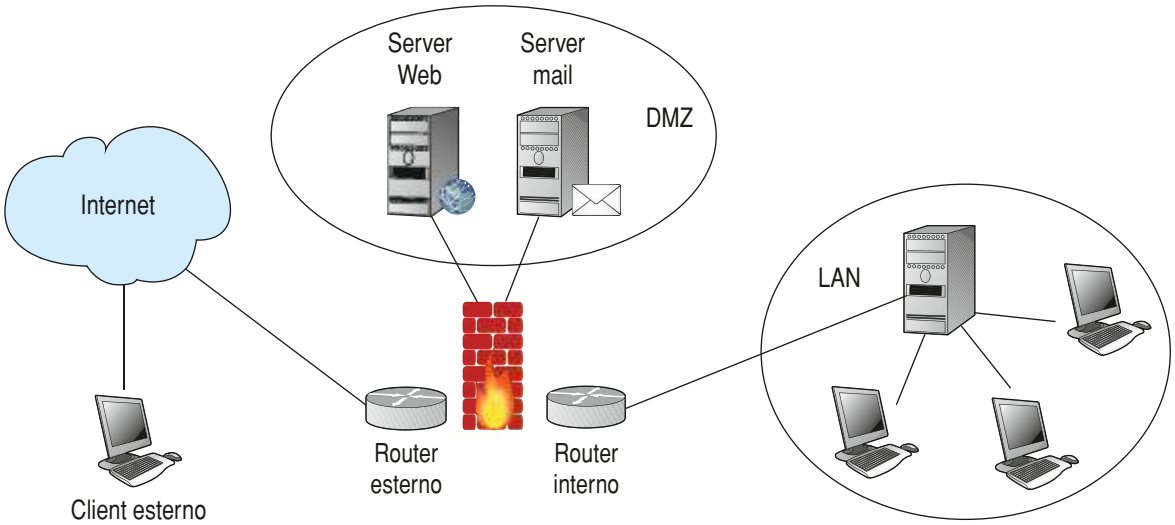
La *principale difesa* contro gli attacchi a una rete è proprio una corretta organizzazione topologica della rete stessa; l'approccio ormai condiviso è quello di suddividere la rete in zone di sicurezza in modo che:

- i dispositivi e le risorse sono posizionati nelle zone in base ai loro livelli e requisiti di sicurezza;
- la rete acquisisce una maggiore scalabilità e una conseguente maggiore stabilità.

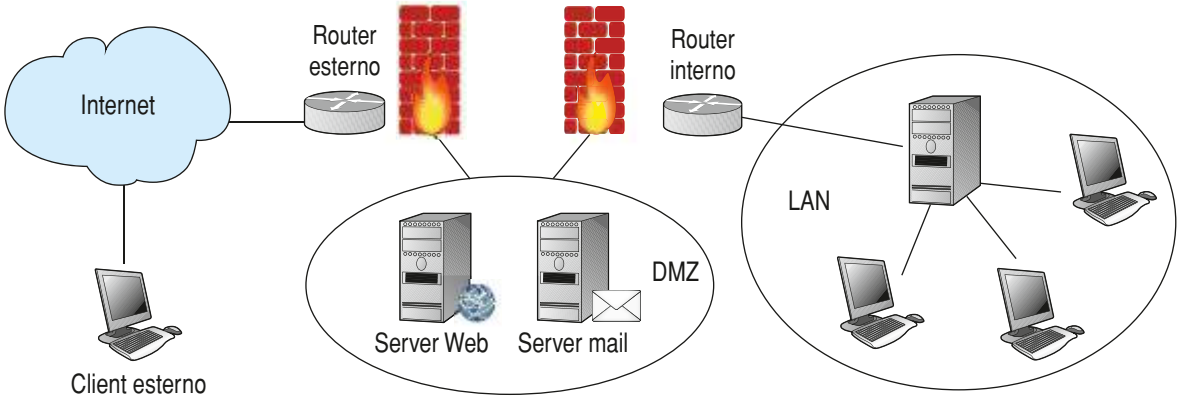
Per essere definita, la DMZ necessita di un IP statico e permette di esporre al WWW un solo indirizzo IP, quindi un solo computer, al quale vengono inoltrate tutte le richieste di connessione.

Abbiamo tre possibili architetture:

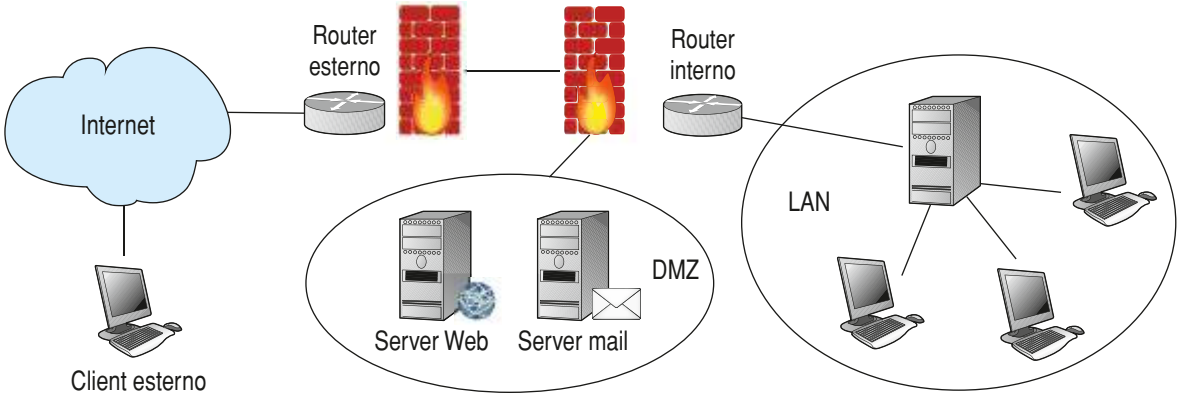
1 DMZ dentro un ramo del firewall



2 DMZ tra due firewall

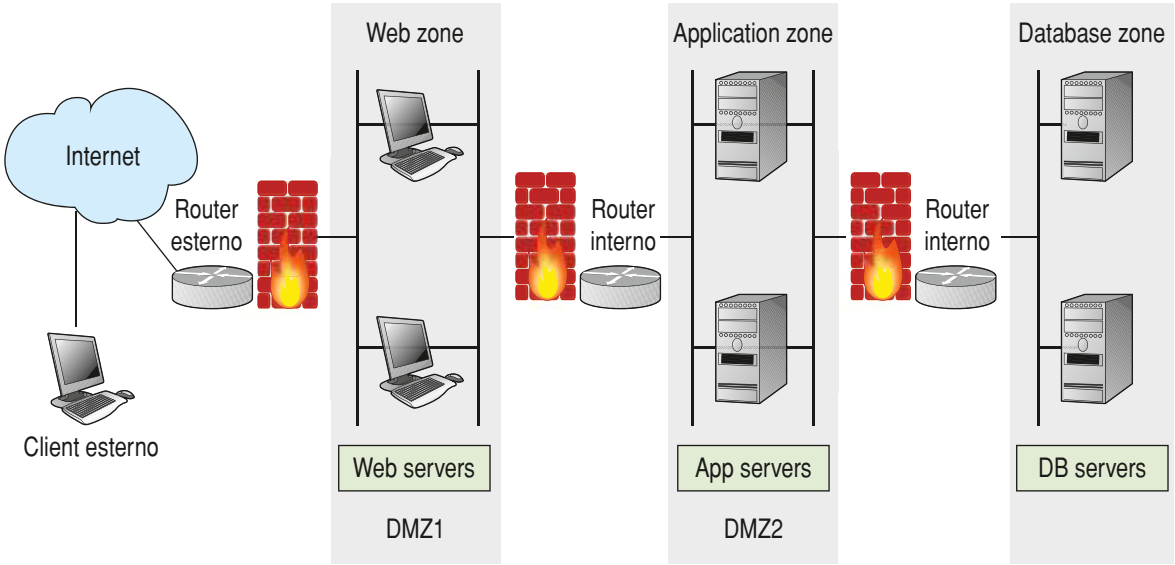


3 DMZ sopra il firewall interno



Utilizzando un'architettura 3-tier (n-tier), dove sono separati Web server, Application Server e il Database, è buona norma mettere il Web server verso l'esterno e collocare nella DMZ l'application Server, che di solito ospita la business logic e si collega al DB, che rigorosamente deve essere all'interno della LAN.

> Nelle ditte in cui la sicurezza dei dati è vitale è possibile introdurre un sistema di stratificazione della DMZ inserendo anche più di due firewalls e più DMZ.



Verifichiamo le conoscenze

1. Risposta multipla

1 L'acronimo ACL deriva da:

a. Access control login
b. Access central list
c. Access control list
d. Access central login

2 Quale tra i seguenti non è un personal firewall?

a. ZoneAlarm
b. Comodo PF
c. Access Limited
d. BlackICE
e. Norton PF

3 I network firewall possono essere classificati in:

a. packet-filtering router
b. router control access
c. circuit gateway
d. proxy server
e. ACL router

4 In un packet filtering router i pacchetti possono essere:

a. accept/allow
b. deny
c. filtered
d. discard/reject

5 Le filosofie alla base delle ACL sono due:

a. accept security policy
b. closed security policy
c. open security policy
d. discard security policy

6 Quale tra i seguenti dati non è presente nella tabella di stato di un firewall stateful inspection?

a. L'identificatore univoco del collegamento di sessione
b. Gli indirizzi IP dell'host sorgente e di destinazione
c. Le interfacce di rete utilizzate
d. L'elenco dei pacchetti accept e deny
e. Lo stato della connessione

2. Vero o falso

1 Un firewall è un sistema hardware-software dedicato alla difesa perimetrale di un host. V F
2 L'application gateway seleziona i pacchetti utilizzando apposite liste di accesso. V F
3 L'egress firewall controlla l'attività del personale interno nella LAN verso l'esterno. V F
4 I personal firewall sono utilizzati in azienda, uno su ogni host. V F
5 Un proxy server fornisce una protezione a livello di applicazione. V F
6 Un packet filtering router scherma i pacchetti dipendentemente dal tipo di protocollo. V F
7 Un packet filtering router analizza le informazioni contenute nell'header TCP/IP. V F
8 Fisicamente il firewall viene disposto su un router di frontiera. V F
9 Un attacco con piccoli frammenti non può essere sconfitto. V F
10 Il packet filtering router permette l'HTTP object caching. V F
11 I firewall stateful inspection effettuano il filtraggio sul singolo pacchetto. V F
12 Un application proxy è in grado di ispezionare l'intera porzione dati del pacchetto. V F

Esercitazioni di Laboratorio 1

INTERCETTARE LA PASSWORD DI POSTA ELETTRONICA CON SNIFF'EM

Il problema degli sniffer

La parola ether della tecnologia Ethernet deriva da "etere" e ogni scheda di rete con tale tecnologia invia il proprio messaggio nell'etere, come altri milioni di utenti: ciascun utente "dovrebbe" essere interessato solo ai messaggi a lui indirizzati e, quindi, dovrebbe ignorare tutti gli altri che sono presenti sulla rete.

Ma se questo è vero per la maggior parte degli utenti: esistono utenti malintenzionati che, invece, si interessano dei dati degli altri per i più disparati motivi.

Un utente malintenzionato può ascoltare illegalmente, o sniffare (questo termine dà più trasgressione all'atto illegale in sé), una sessione di posta in uscita tra un utente e il suo server di posta utilizzando proprio la caratteristica di tali schede con tecnologia Ethernet, che non offrono la benché minima sicurezza.

Oltre a Wireshark, già descritto nell'unità di apprendimento 4 del volume 2 (lab. 3), in questa lezione descriveremo le caratteristiche essenziali di un altro pacchetto, lo Sniff'em che, proprio come dice il nome, è cioè Sniffer email, è particolarmente indicato per effettuare lo sniffing della posta elettronica.

Sniff'em

Il programma Sniff'em dimostra quanto insicura possa essere una rete con tecnologia Ethernet: con esso si possono intercettare tutti i dati in transito e quindi letti senza permesso alcuno del mittente o del destinatario.

Ma Sniff'em viene usato nell'ambito della sicurezza informatica per molti "scopi legali", grazie alla sua particolare versatilità: dall'analisi dei pacchetti catturati si può capire se esistono eventuali problemi di collegamento tra due computer in una rete locale, oppure verso un server Internet, indipendentemente dal protocollo utilizzato.

> Con Sniff'em si possono analizzare i pacchetti anche con lo scopo di scoprire dove c'è una falla nella sicurezza, soprattutto nei casi in cui viene richiesta la riservatezza, e verificare se questi viaggiano in modalità criptata, e quindi sicura, o meno.

Non è però un prodotto completamente gratuito: permette di effettuare le operazioni solo "sui dati in uscita e ignorerà i dati in arrivo": ma questo non limita il suo funzionamento e permette di capirne le potenzialità.

È anche possibile avere una versione demo full-duplex per un periodo limitato: contattare demo@sniff-em.com per ulteriori informazioni.

Caratteristiche

Riportiamo le caratteristiche così come sono dichiarate dal produttore.

Here are some features highlights within Sniff'em:

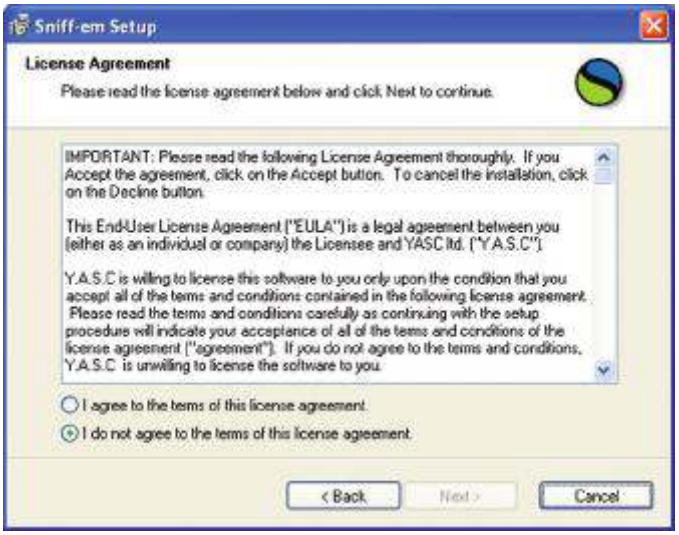
- it proactively monitor network traffic organization retrace the exact steps of any network user;
- inform yourself Instantly of ANY hack/crack and infiltration attempts;
- automatic advanced decoding of DNS, and Netbios Packets;
- special Logging Modes aimed at the automatic logging of all/or rule-based filtered Traffic through a given Network;
- buffer Decoding (Supported: TCP, TELNET, HTTP, POP3, SMTP, AUTH, IRC, DOMAIN, FINGER, FTP, FTP-DATA....);
- Sniff'em boasts incredibly easy to use user friendly interface, designed with productivity in mind;
- many ways to edit / create packages (with package details or PacketView itself);
- able to detect over 171 HighLevel Protocols;
- the Detailed Packet View Decodes (ARP, IP (TCP, UDP, ICMP, IGMP), PPP (PAP, ATCP, BCP, BVCP, PCC, DNCP, ECP, IPCP, IPV6CP, IPXCP, NBFCP, OSINLCP, SDCP, SNACP, XNSCP , BACP, BAP, CHAP, EAP, LCP) packets and displays them in a nice way;
- decoded and Packet data are modifiable on the fly;
- encryption of saved Projects/Log files;
- anti-Tampering features.

Installazione

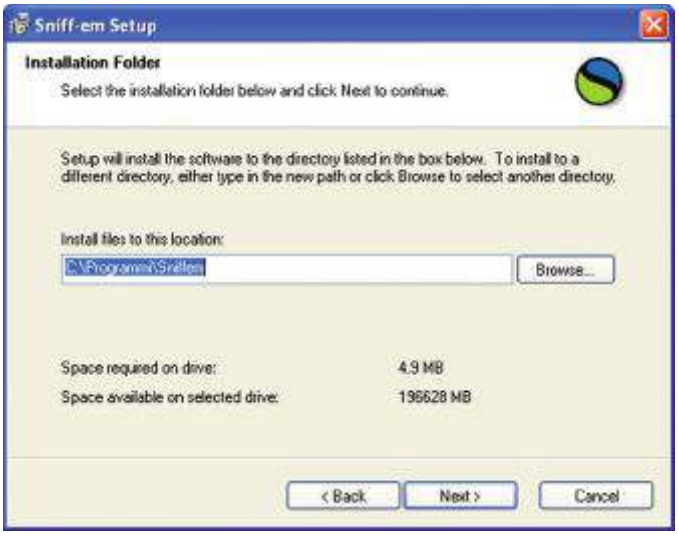
Il download può essere effettuato da diversi indirizzi tra cui http://sniff-em.software.informer.com/1.1/ è possibile scaricare il programma installatore del sito www.hoepliscuola.it nella cartella materiali della sezione riservata a questo volume.

Avviando il programma di installazione di Sniff'em la prima videata di setup è la seguente: ▶

Si prosegue come al solito con l'accettazione della licenza d'uso: ▶



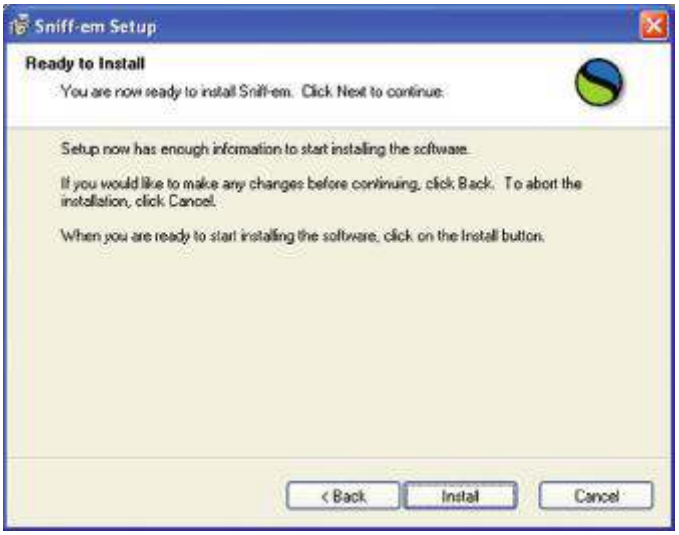
Si procede confermando la directory di installazione: ▶



Si definisce quindi la short-cut di accesso rapido: ▶

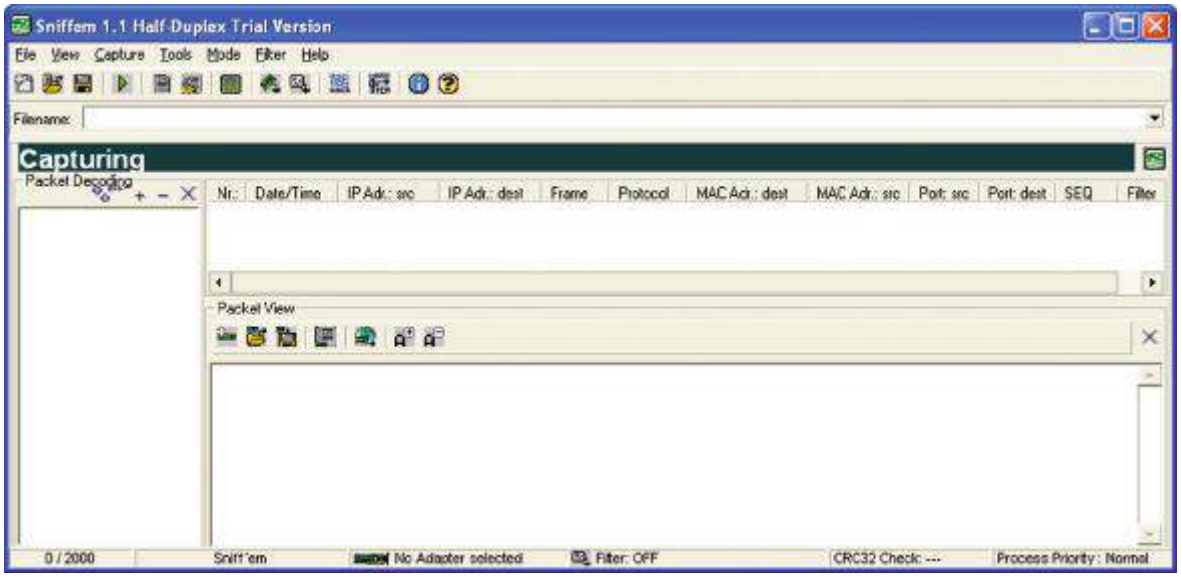
E quindi inizia la vera e propria installazione. ▶

Al termine è necessario riavviare il computer.



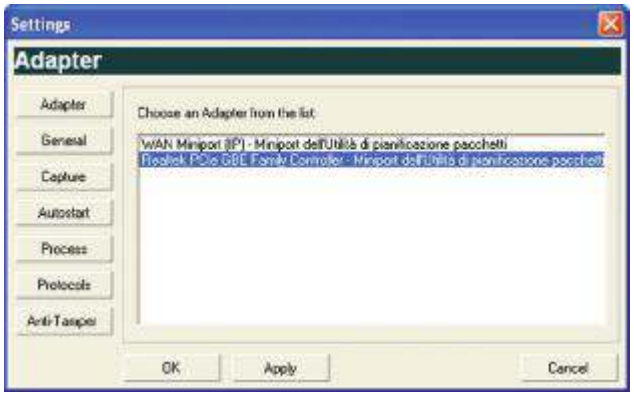
Avvio del programma

Al suo primo avvio Sniff'em si presenta con la seguente videata:

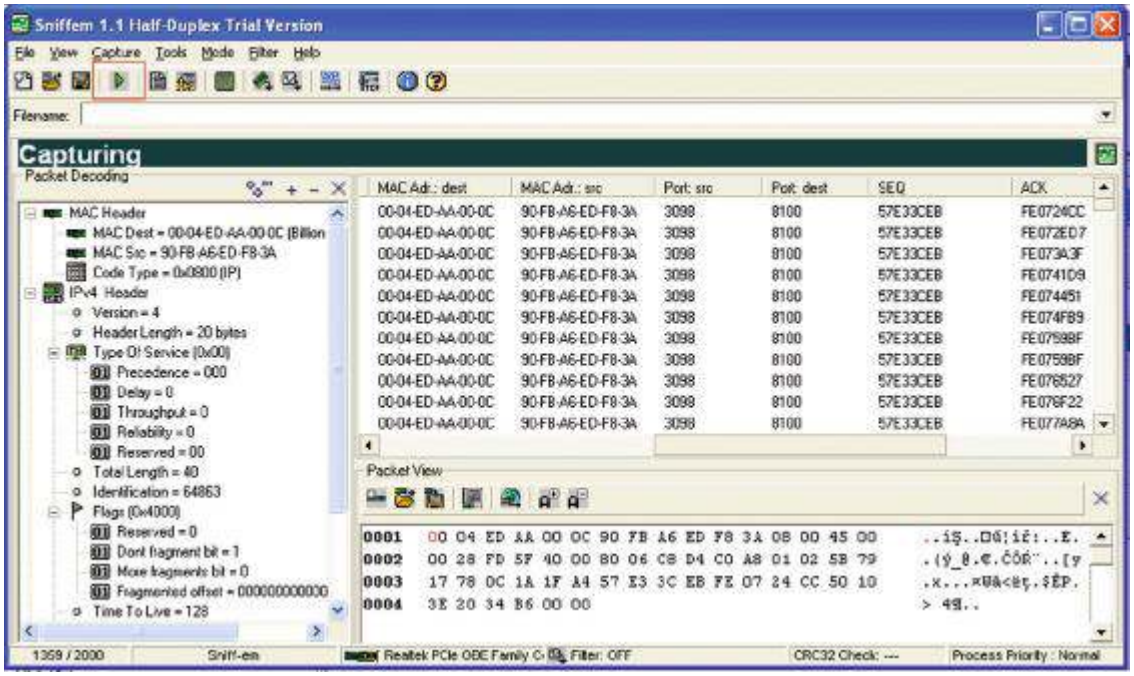


Per prima cosa è necessario effettuare la configurazione:

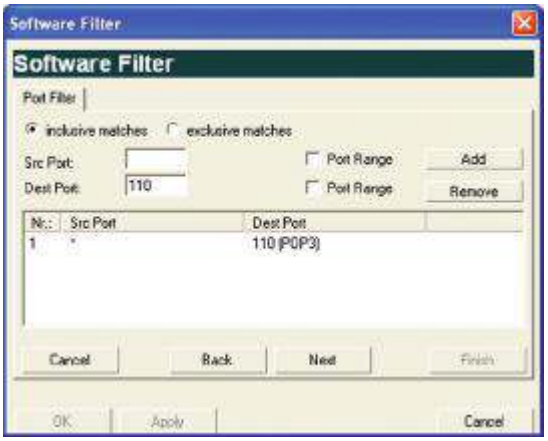
Incominciamo dall'adattatore, cioè selezioniamo l'interfaccia sulla quale deve "porsi in ascolto":



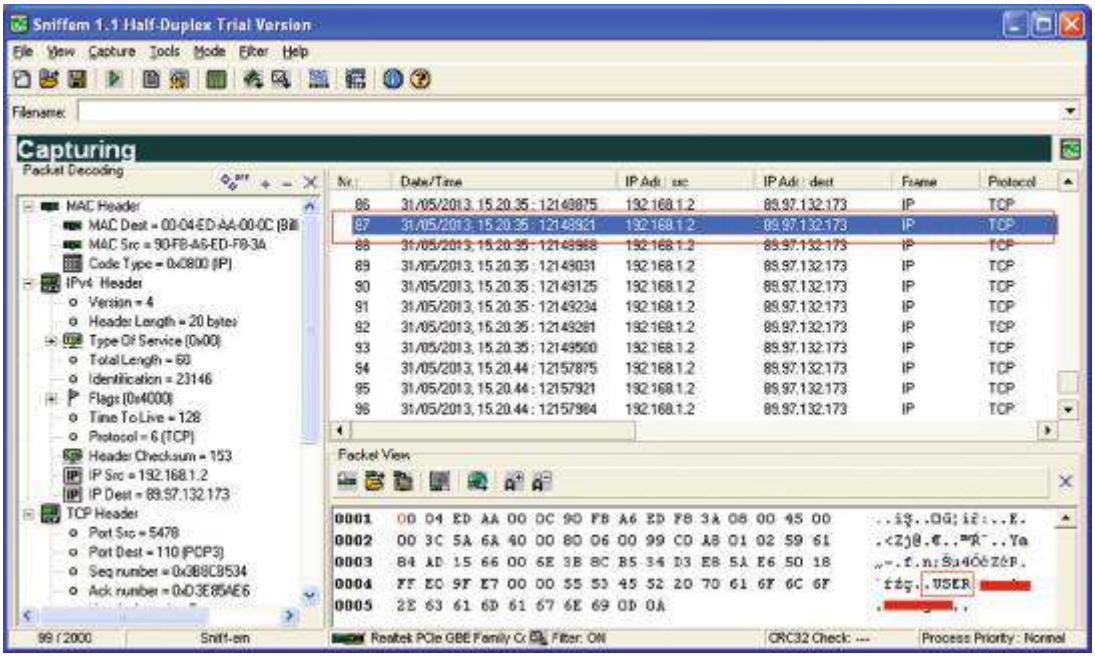
Iniziamo la cattura dei pacchetti cliccando sul tasto verde del menu a icone e subito verranno visualizzati i pacchetti "sniffati":



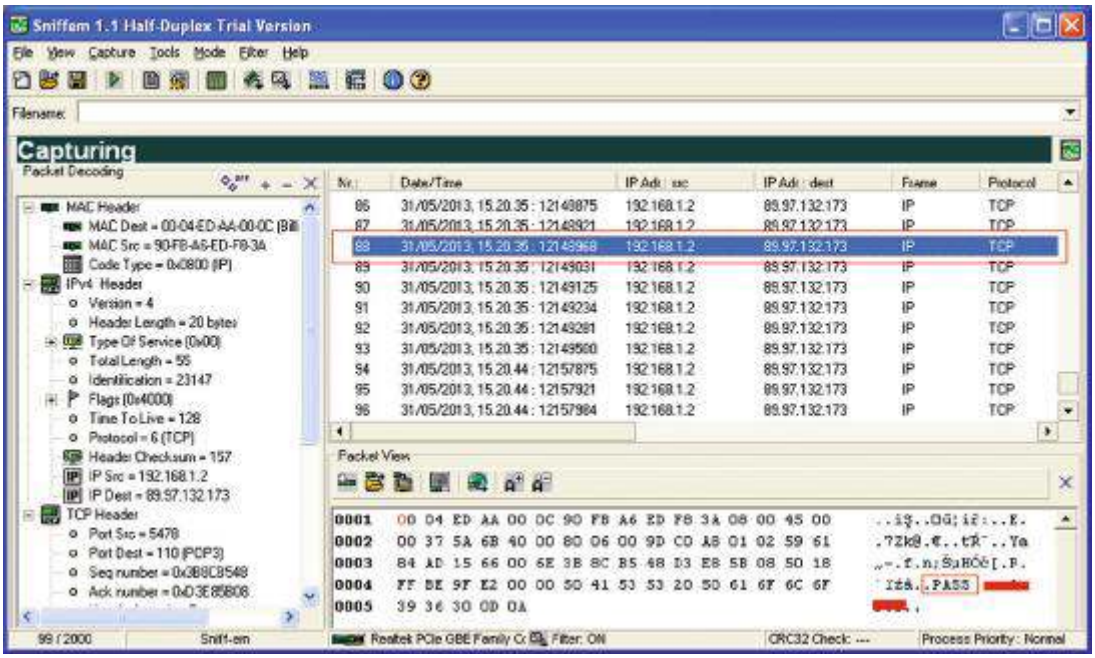
Scriviamo una email e intercettiamone i pacchetti, magari inserendo un filtro per meglio identificare quelli di nostro interesse:



La versione free intercetta solo messaggi in uscita, quindi spediamo un messaggio di prova, ad esempio da MS Explorer e verrà visualizzato un insieme di pacchetti:

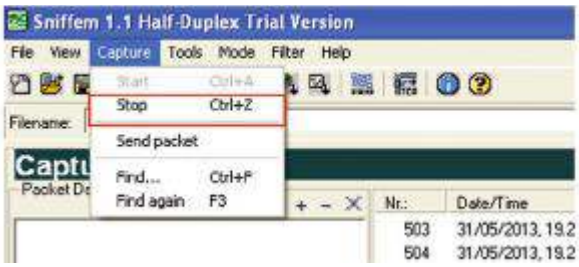


Ogni pacchetto viene numerato ed etichettato con data e ora rendendolo facilmente individuabile anche grazie alla visualizzazione degli indirizzi IP del mittente e del destinatario: posizionandoci sul pacchetto 87 nella finestra inferiore etichettata con Packet View si possono vedere i byte in formato ASCII ed è facilmente individuabile il nome dell'utente (USER, qui cancellato per motivi di privacy).



Nel pacchetto successivo è facilmente individuabile la password (PASS, qui cancellata per ovvi motivi): quindi le informazioni riservate sono state intercettate e "sniffate" da questo programma.

Si termina la cattura dei pacchetti cliccando sempre sull'icona oppure dalla corrispondente opzione della tendina capture.



Prova adesso!

- Applicare le tecniche di sniffing delle email

Scrivi una mail e intercettala individuando la USER, la PASS e il testo inviato.
Nella finestra di sinistra etichettata Packet Decoding sono dettagliati tutti i singoli byte del pacchetto.
Analizza byte per byte costruendo una tabella come quella di figura per il pacchetto che contiene USER e per quello che contiene la PASS:

Nr. Byte	Significato	Dettaglio	Valore HEX	Valore ASCII
1-7	MAC HEADER	MAC destinatario	00 04 ED ZZ 00 0C	<non significativo>
…				
…				
…				

Esercitazioni di Laboratorio 2

IL PACCHETTO PGP DESKTOP

PGP Desktop

PGP Desktop 9.02 utilizza una cifratura a chiave simmetrica e una cifratura a chiave asimmetrica per garantire la riservatezza: la versione che noi utilizzeremo, cioè l'evaluation version, ha le funzionalità limitate, ma ci permette comunque di valutarne le possibilità.

> "PGP" e "Pretty Good Privacy" sono marchi registrati, e il logo PGP è un marchio di fabbrica, di PGP Corporation negli Stati Uniti e in altri paesi. "IDEA" è un marchio di Ascom Tech AG. L'algoritmo di crittografia IDEA descritta nel brevetto statunitense numero 5.214.703 è concesso in licenza da Ascom Tech AG.
> L'algoritmo di crittografia CAST è concesso in licenza da Northern Telecom, Ltd.

PGP Desktop 9.02 è il primo prodotto basato su server che è il "robot messaggero sicuro" ed è molto semplice da utilizzare in quanto, una volta definite le chiavi, automaticamente si occupa di gestire la posta in ingresso e in uscita.
PGP Desktop 9.02 ha una semplice interfaccia utente (UI) che permette di accedere alle chiavi e ai certificati in modo da poter modificare tutti i campi e anche selezionare gli algoritmi di cifratura che si desiderano utilizzare, impostare un server di chiavi di default, e così via.
Si può impostare PGP Desktop in modo che esegua automaticamente la scansione del corpo del messaggio per individuare messaggi crittografati e/o firmati, così come è anche possibile impostarlo in modo che ogni volta che si inviano messaggi a certe persone o domini, sarà cifrato o firmato automaticamente.
È anche possibile crittografare il disco rigido, completamente o parzialmente creando PGP virtual Disk.

Installazione

Per poter effettuare l'installazione è necessario scaricare il file e scompattarlo utilizzando un qualsiasi programma compatibile con l'algoritmo di compressione zip, ottenendo due file:

- PGPDesktop902_Inner.exe: il programma di installazione vero e proprio;
- PGPDesktop902_Inner.exe.sig: la firma associata al programma necessaria per verificarne l'integrità e la provenienza.

> Il file compresso è scaricabile dalla cartella materiali della sezione del sito www.hoepliscuola.it riservata a questo volume.

Per effettuare l'operazione è necessario aver installato una precedente versione di PGP e che all'interno del proprio portachiavi pubblico vi sia almeno la chiave pubblica di Phil Zimmermann.

Avviamo la procedura di installazione eseguendo il programma PGPDesktop902_Inner.exe: cliccando l'icona come primo passo è necessario selezionare la lingua:

Si accetta la licenza d'uso:

Dopo aver letto le informazioni relative alla versione che stiamo installando:

Si procede con l'installazione dei file sul computer:

Fino a che viene presentata la videata finale che richiede il riavvio del PC.

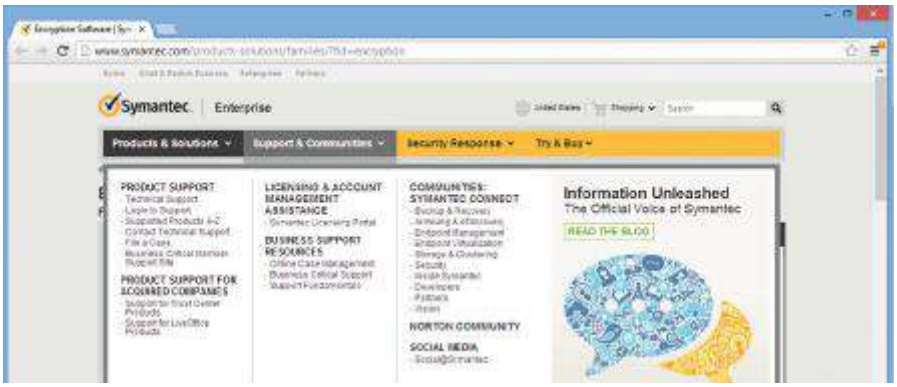
PGP setup

Al riavvio del computer si avvia automaticamente una fase di setup, che inizia abilitando l'utente corrente all'utilizzo del prodotto:

Si procede con il completamento dei dati per ottenere una licenza d'uso del prodotto:

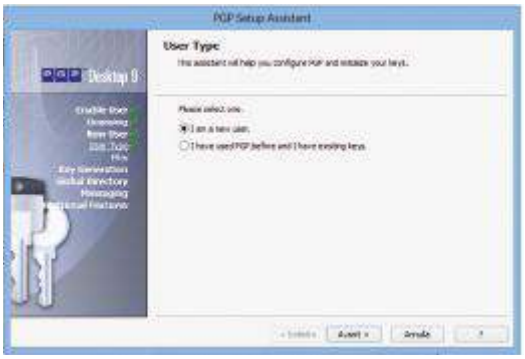
È possibile inserire il numero di licenza per attivare le funzionalità complete del prodotto oppure richiedere una licenza trail di 30 gg:

Richiediamo ora la licenza di prova, seguendo le indicazioni del sito della Symantec:



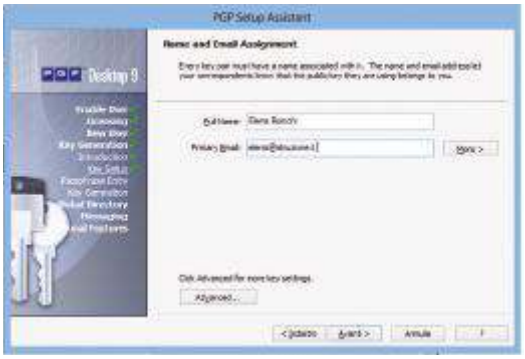
In attesa che ci venga comunicato per email il numero di licenza, procediamo selezionando l'ultima opzione che ci attiva solo opzioni mostrate a fianco.

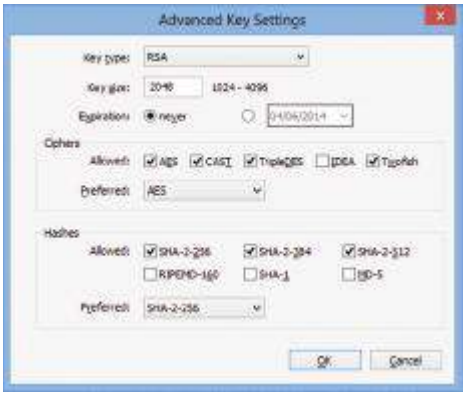
Ora procediamo con la generazione delle chiavi:



Confermiamo che siamo dei nuovi utenti:

Inseriamo il nostro nome e l'indirizzo di email:

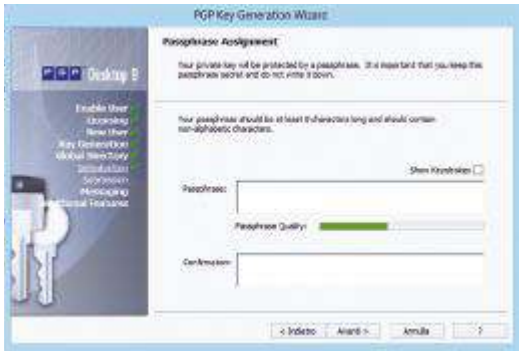




Se clicchiamo su Advanced è possibile selezionare le impostazioni della chiave:

- tipo di chiave: scegliere tra Diffie-Hellman/DSS e RSA;
- dimensione della chiave: il range è compreso tra 1024 bit e 4096 bit; maggiore è la chiave e maggiore è la sicurezza ma ci vorrà più tempo per cifrare (la dimensione standard è 1024);
- scadenza: selezionare Mai o specificare una data in cui cesserà la validità della coppia di chiavi;
- crittografie ammesse: deselezionare i cifrari che non siano supportati dalla coppia di chiavi che si sta creando;
- cipher preferita: selezionare il cifrario che si desidera utilizzare;
- hash ammessi: deselezionare gli algoritmi di hash che non si vuole siano supportati dalla coppia di chiavi che si stanno creando;
- hash preferita: selezionare l'hash che si desidera utilizzare.

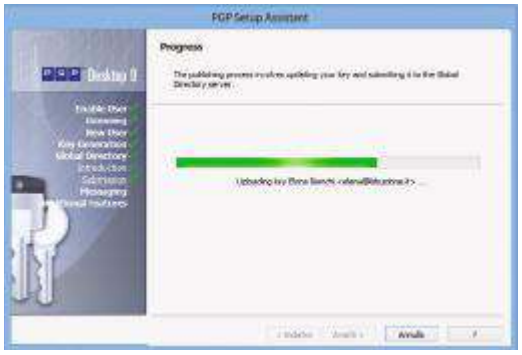
Confermiamo le scelte con OK e proseguiamo con la definizione della passphrase di protezione della nostra chiave:



Alla conferma avviene la generazione:

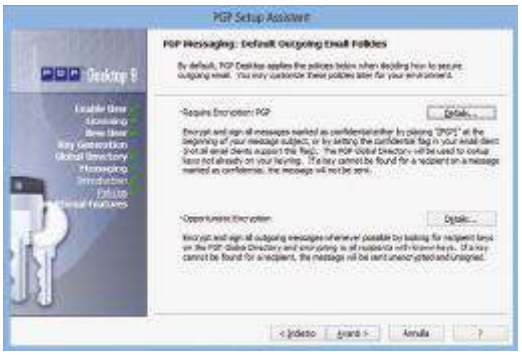
La nostra chiave deve essere distribuita: questo avviene automaticamente dal PGP Global Directory assistant.

Avviando l'esecuzione dopo qualche secondo termina la procedura.



La gestione della posta elettronica avviene in automatico: avviamo la procedura che effettua il riconoscimento del nostro account di posta:

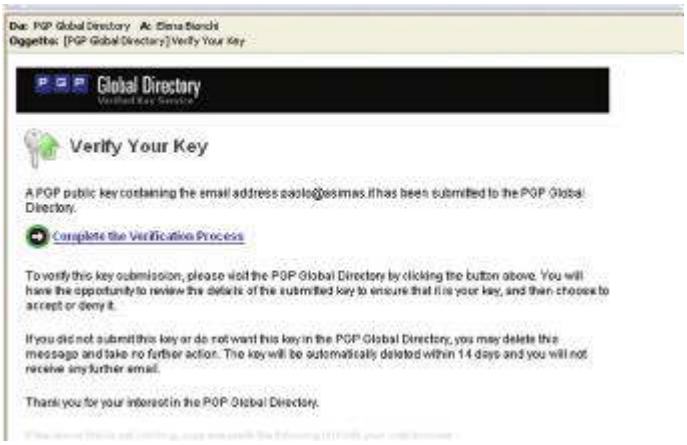
e definisce le politiche di gestione, che accettiamo così come sono configurate di default.



Per poter utilizzare questa funzionalità è necessario avere la licenza del prodotto completo (anche in versione evalutation copy).

Al termine del setup ci viene mostrata l'icona di avvio del programma, posizionata nel system tray e quelle del "distruttore di documenti segreti", posizionata sul desktop.

Prima di iniziare a utilizzare PGP è necessario completare il processo di verifica della chiave – indirizzo di posta rispondendo alla mail che nel frattempo ci è stata inviata da PGP:



Cliccando sul link viene richiamata la pagina Web che ci richiede di confermare la chiave e l'indirizzo di email:

Possiamo ora scaricare la chiave e iniziare a utilizzarla.

Vengono generate le due chiavi, che sono file, secring.skr, e pubring.pkr, archiviate di default nella cartella Documenti.
Attenzione: nella terminologia PGP, ogni voce del keyring pubblico è un certificato della chiave pubblica.

Primo utilizzo di PGP

Dopo aver riavviato il computer è possibile avviare PGP Desktop tramite l'icona di figura posizionata nel ◀ system tray ▶ (può essere o un lucchetto chiuso isolato oppure come un lucchetto chiuso collegato a un cavo di rete): cliccandola viene visualizzato il menu che permette di effettuare le principali opzioni del prodotto.

◀ Il system tray è quella porzione di schermo che si trova a destra della barra delle applicazioni e a sinistra dell'orologio di sistema. ▶

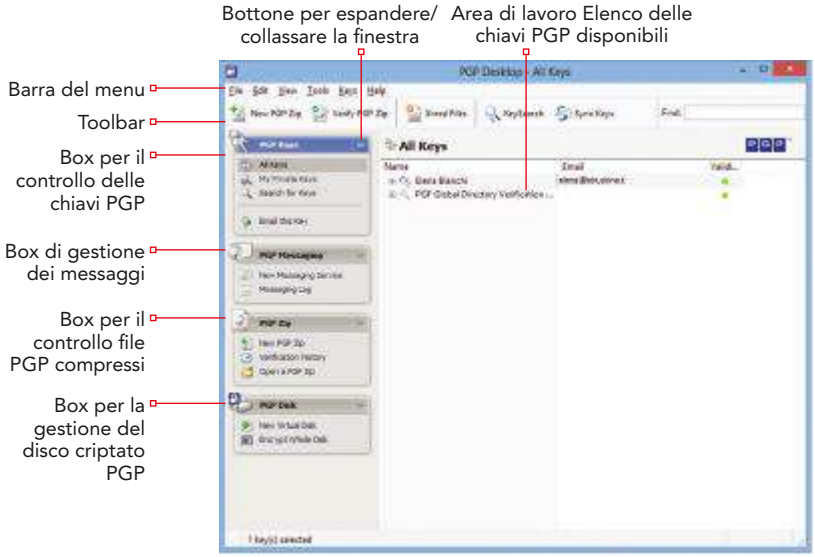
Per prima cosa clicchiamo su About PGP Desktop: ▶

viene visualizzata la versione del prodotto e ci permette di accedere alla licenza: ▼

Dal 2010 i diritti su PGP sono stati acquisiti dalla Symantec e quindi parte delle funzionalità non sono attivate in quanto non sono gratuite; è però possibile avere una licenza trial di 30 giorni per poter valutare appieno le potenzialità del prodotto:

Da qui è possibile modificare le condizioni di licenza: attendiamo che ci giunga la mail da Symantec per poi introdurre il codice temporaneo che ci permetterà di utilizzare per 30 giorni il prodotto completo.

Clicchiamo ora nella tendina l'opzione Open PGP Desktop che ci avvierà la videata generale del programma, dove abbiamo indicato gli elementi principali:



Descriveremo le diverse opzioni man mano che verranno utilizzate.

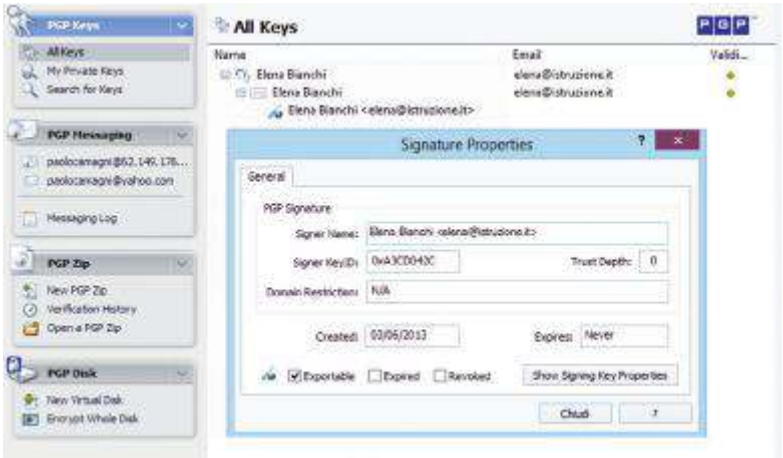
Gestione chiavi (keyring)

Il primo box permette la completa gestione delle chiavi; di default sono presenti tre viste:

- All Keys: mostra tutte le chiavi PGP presenti;
- MY Private Keys: mostra solo le chiavi private nel portachiavi (keyring) personale;
- Search for Keys: permette di cercare le chiavi sul vostro portachiavi in base a diversi criteri.

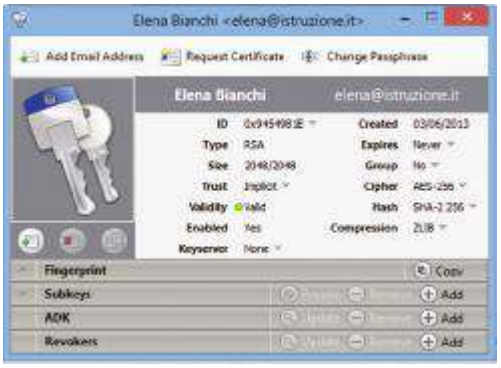
Cliccando su All Keys vengono visualizzate due chiavi attualmente presenti: quella di PGP e la nostra, appena creata e validata (nel mio caso *Elena Bianchi*). Selezioniamo la nostra Key, che viene descritta su tre diversi livelli, espandibili selezionando il simbolo +:

- 1° livello: nome, cognome, email principali del proprietario;
- 2° livello: è possibile associare al proprietario diversi ID, ciascuno associato a un nome e un indirizzo email: avere ID diversi permette all'utente di specificare identità e indirizzi email diversi;
- 3° livello: contiene le firme che convalidano quell'ID, dove ogni ID può essere convalidato da una o più firme che stabiliscono la certezza che la chiave appartenga all'ID corrispondente (=validity dell'ID). Se convalidiamo un ID di un utente con la nostra firma, a quell'ID viene assegnato automaticamente il massimo livello di certezza.

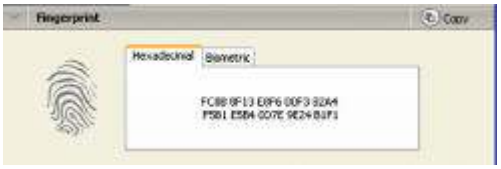


Un doppio clic sul nome del proprietario della chiave permette di visualizzare la finestra con i dati generali della Key: ▶

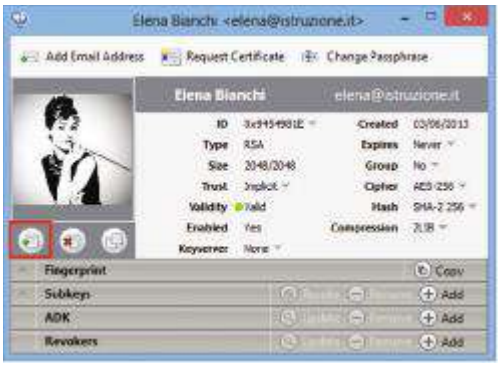
Per vedere le proprietà si clicca su Show Signing... e si ottiene:



E possiamo anche visualizzare l'impronta digitale:



È possibile modificare il profilo aggiungendo una immagine.

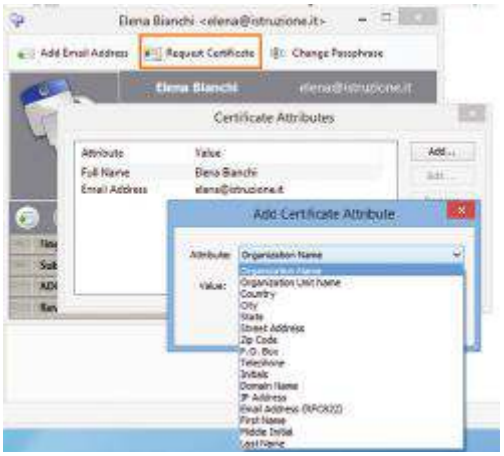


I principali campi sono:

- Validity: indica con un pallino verde/ grigio il livello di certezza che la chiave appartenga al proprietario specificato: il campo Validity è associato sia al 1° livello (=proprietario) sia al 2° livello (=ID) del campo Key: se a firmare la chiave sono io, cioè il proprietario del keyring, il pallino diventa automaticamente verde, cioè chiave valida;
- Trust: indica il livello di fiducia nella persona che possiede quella chiave pubblica: una chiave firmata (=validata) da un utente *trusted* non richiede che io firmi a mia volta la chiave per validarla.

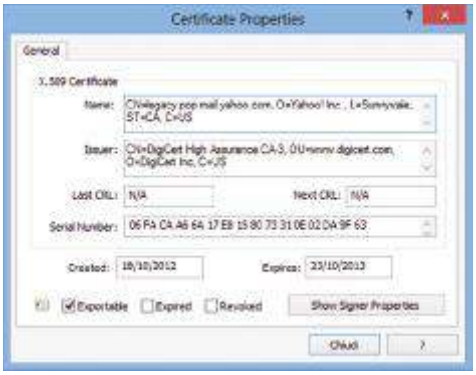
> Questo meccanismo permette di creare reti di fiducia delegando l'attestazione di fiducia a un altro utente al quale sia già stato associato un trust.

È possibile richiedere un certificato completando i campi come si può vedere dalla successiva schermata:



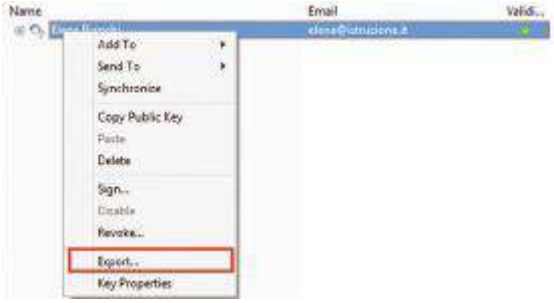
La licenza di valutazione non permette di gestire automaticamente le email: è invece possibile sia cifrare i file singolarmente sia le intere directory e cifrare tutto il disco oppure una parte di esso.

È possibile visionare le caratteristiche del certificato:



Importazione chiave pubblica degli utenti con cui comunicare

Per poter comunicare in modalità criptata è necessario che mittente e destinatario siano in possesso delle stesse chiavi, cioè delle proprie chiavi pubbliche. Scambiarsi le chiavi pubbliche è facile: c'è un'opzione Export nel menu che viene visualizzato cliccando col tasto destro sulla chiave



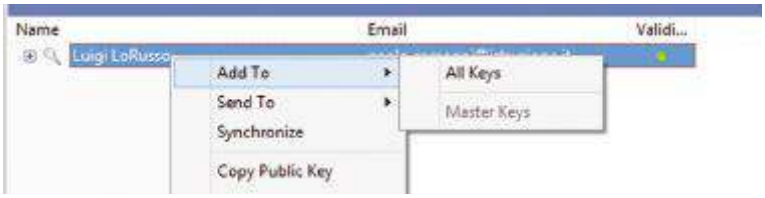
che permette di creare un file .asc che si può distribuire pubblicamente e contiene la chiave pubblica dell'utente.

> È possibile esportare tutte le chiavi presenti nel nostro PC, quindi non solo la nostra ma anche quella dei nostri contatti.

Per importare, selezionare Import sotto il menu Keys.

È anche possibile ricercare Keys di persone alle quali vogliamo comunicare in modo criptato direttamente nel database di PGP: la ricerca può essere fatta sia per nome che per indirizzo di email.

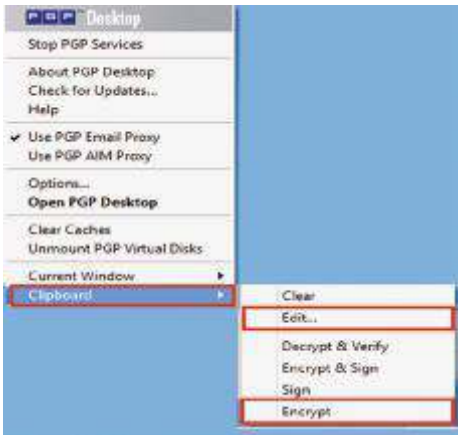
Cliccando col tasto destro sulla chiave trovata ci si presenta il menu con le diverse opzioni: aggiungiamo la chiave al nostro "portafoglio delle chiavi" in modo da poterla utilizzare per inviare i messaggi criptati al *nostro amico.*



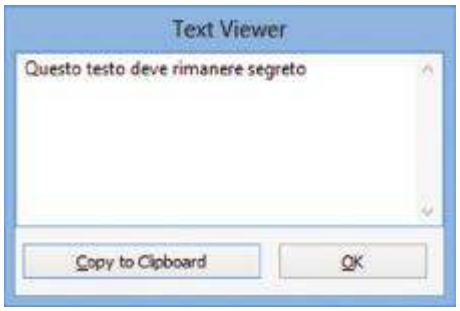
Ora abbiamo questa situazione, dove sono presenti due chiavi pubbliche che possono essere utilizzate per la gestione delle email protette.

Cifrare una frase

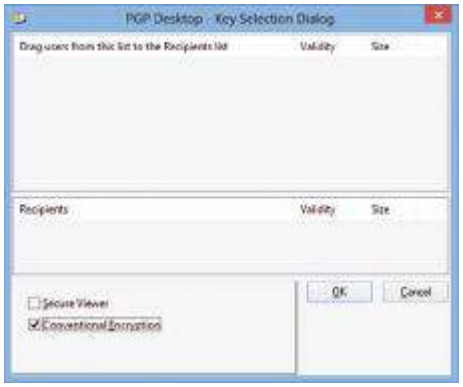
Selezioniamo da System Tray l'icona del lucchetto (PGPtray) e nel menu che ci verrà proposto selezioniamo Clipboard > Edit ...



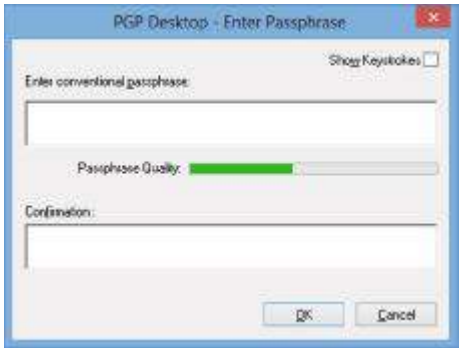
scriviamo un testo e copiamolo nella Clipboard:



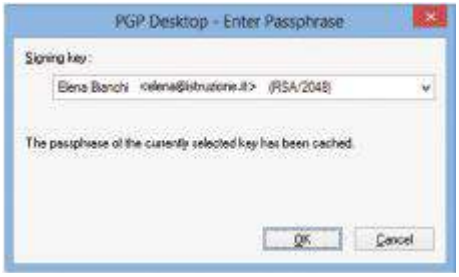
Quindi sempre dalla stesso menu selezioniamo Encrypt e nella successiva finestra spuntiamo il check Conventional Encryption e confermiamo con OK:



Ora ci viene richiesta la passphrase: scriviamola due volte, negli appositi textbox:



Scegliamo ora su quale chiave associare la passphrase: dato che ne abbiamo solo una, la scelta è automatica:



Il processo termina con OK.
Se ora rientriamo, selezioniamo Clipboard > Edit ... e troviamo la nostra frase criptata:

Selezioniamo dal menu ora l'opzione Decrypt/Verify: ci viene richiesto di inserire la passphrase per poter effettuare la decriptazione:

Otteniamo la seguente videata:

Prova adesso!

• Criptare frasi con PGP Desktop

Ripeti la procedura qui descritta selezionando l'opzione sign al posto di encrypt: quindi prova a utilizzare tutte le opzioni presenti nel menu Clipboard.
Analogamente prova a utilizzare tutte le altre opzioni del menu Current Window, e cioè ▶:

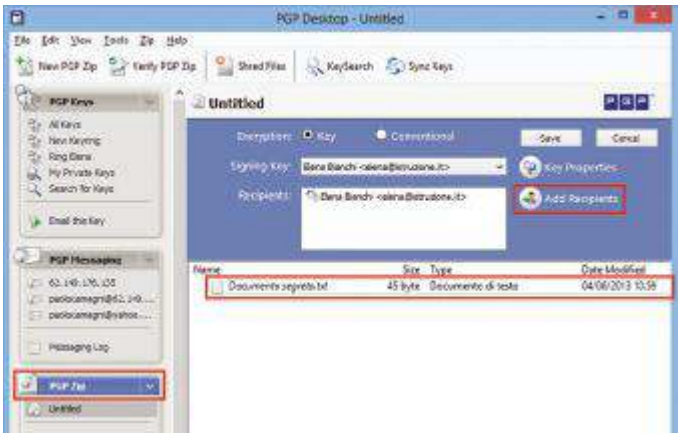
PGP Messaging: cifrare un messaggio di posta elettronica

Questa funzionalità è disponibile solo se si è in possesso di una licenza completa: descriviamo i semplici passi da effettuare con un programma di posta elettronica (ad esempio MS Outlook Express).

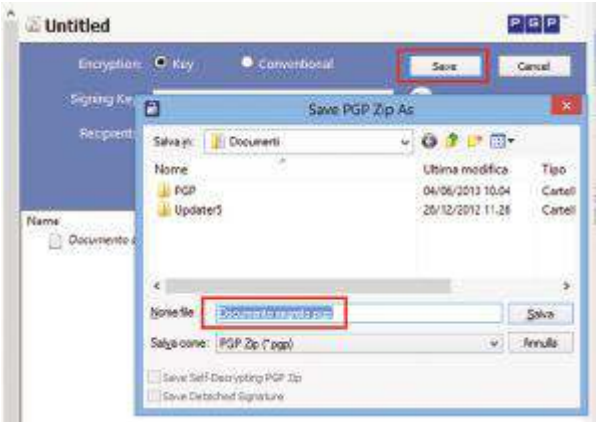
1. Si avvia MS Outlook Express.
2. Si scrive un nuovo messaggio di posta utilizzando l'apposita opzione del menu File oppure l'icona corrispondente nella barra degli strumenti.
3. Si seleziona l'icona nella barra degli strumenti contenente una busta e un lucchetto di colore oro.
4. Quindi si compila il messaggio selezionando il destinatario del destinatario del messaggio cifrato, l'Oggetto e il Corpo.
5. All'invio del messaggio questo verrà automaticamente cifrato da PGP Desktop.

PGP Zip

Il box PGP Zip permette di generare dei file compressi e criptati: dopo aver selezionato la Key e un contenitore con l'opzione Add Recipient, si trascinano nell'area di lavoro i file che si vogliono criptare e cifrare:



Quindi si conferma con Save e si sceglie il nome del file .pgp e la destinazione (di default viene proposta la cartella documenti):



Se si prova ad aprire il file creato con un editor si visualizza una situazione simile alla seguente:

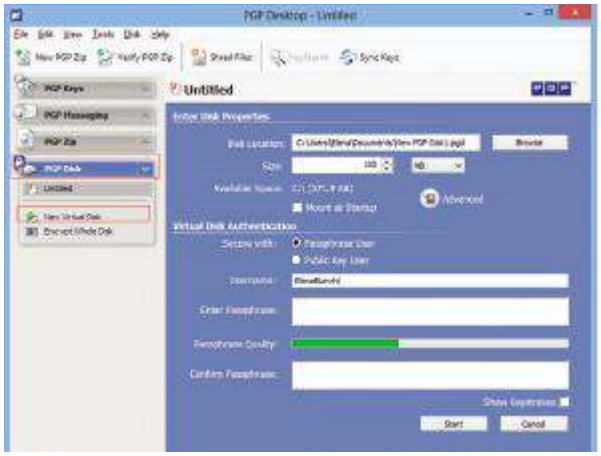
È naturalmente possibile aggiungere più di un file a un archivio PGPZip:

Name	Size	Type	Date Modified
Documento segreto.txt	45 byte	Documento di testo	04/06/2013 11.10
Lista della spesa.txt	19 byte	Documento di testo	04/06/2013 11.10

In Italic (corsivo) viene visualizzato il file che non è ancora stato salvato: procediamo salvandolo in un nuovo file DueDocumenti.pgp: ora sullo schermo viene visualizzata la seguente videata:

■ PGP Disk

È possibile creare un volume (o più volumi) cifrato semplicemente selezionando dal box PGP Disk l'opzione New virtual disk:



Dopo aver assegnato un nome al volume e stabilito la dimensione, basta inserire la propria Key per avviare la "formattazione cifrata" del volume che, però, senza la licenza completa, non è abilitata.

Prova adesso!

- Applicare il programma PGP Desktop

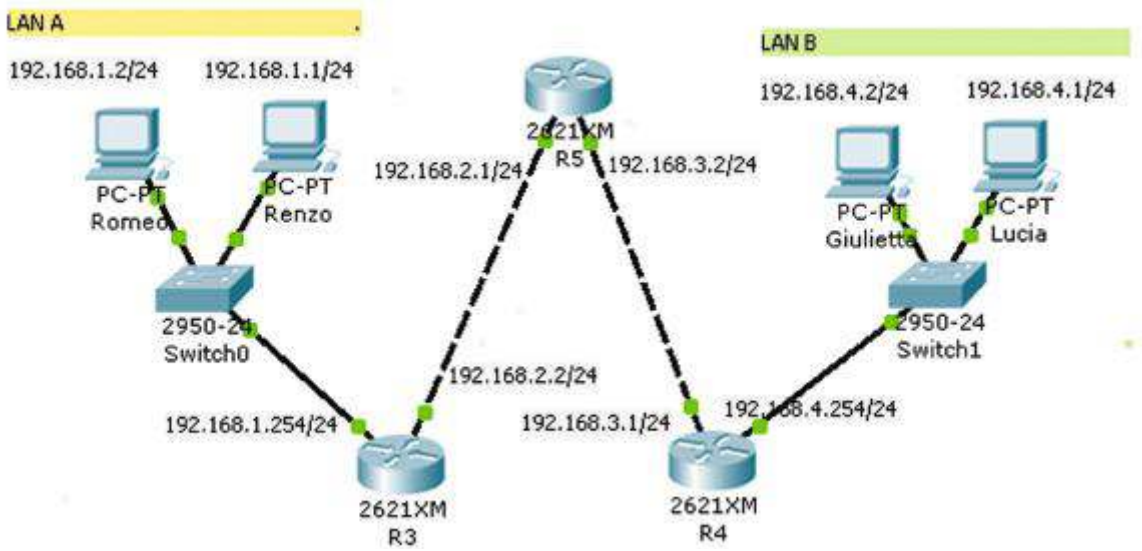
Dopo aver richiesto la licenza provvisoria e abilitato il programma completo.

1. Realizza due dischi virtuali:
   - Adamo.PGP con dimensioni 100 Mb, algoritmo AES (256bit) con file sytem FAT;
   - Eva.PGP con dimensioni 100 Mb, algoritmo Twofish (256bit) con file system NFTS.
2. Confronta i tempi impiegati per la cifratura dei due dischi.
3. Salva lo stesso file di testo in entrambi i dischi: cosa puoi osservare?

Esercitazioni di Laboratorio 3

REALIZZIAMO UNA VPN CON PACKET TRACER

Per poter definire una VPN è necessario avere a disposizione una rete sulla quale operare: realizziamo quella riportata nella figura seguente:



Per la LAN A connettiamo due PC a uno switch, con la seguente Addressing Table:

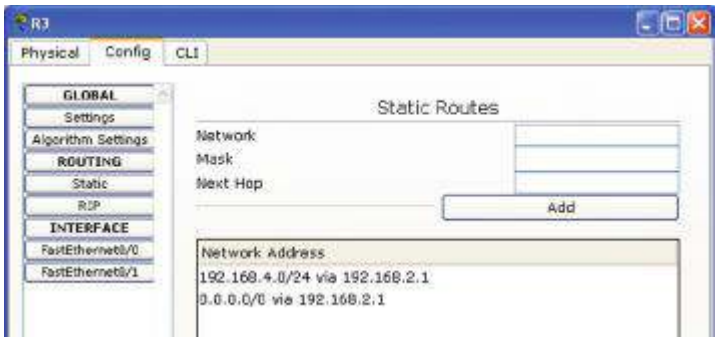
Device	IP Address	Subnet Mask	Default Gateway
Romeo	192.168.1.2	255.255.255.0	192.168.1.254
Renzo	192.168.1.1	255.255.255.0	192.168.1.254

Per la LAN B connettiamo due PC a uno switch, con la seguente Addressing Table:

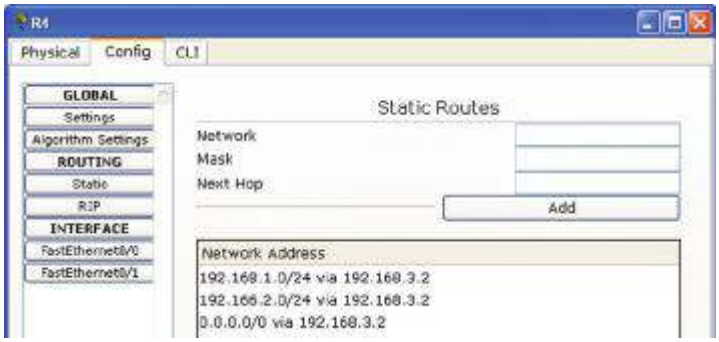
Device	IP Address	Subnet Mask	Default Gateway
Giulietta	192.168.4.2	255.255.255.0	192.168.4.254
Lucia	192.168.4.1	255.255.255.0	192.168.4.254

La configurazione dei router non richiede particolari accorgimenti: riportiamo per comodità solo le tabelle statiche.

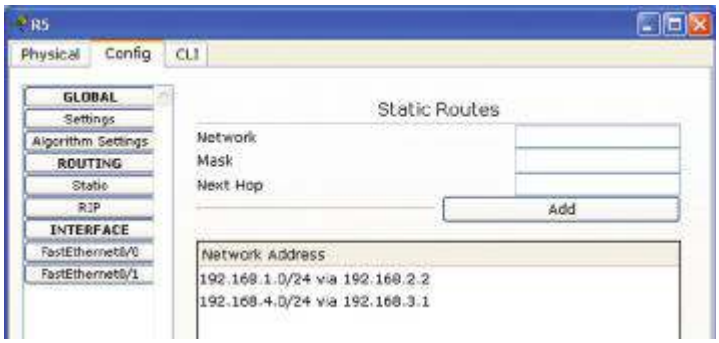
Router R3



Router R4



Router R5



■ VPN – crittografia

Dopo avere collaudato il funzionamento della rete verificando che i pacchetti della rete LAN A giungano alla LAN B, procediamo con la creazione di un tunnel tramite il quale i pacchetti scambiati tra il router r3 e il router r4 vengano cifrati, così da garantire l'integrità e la riservatezza delle comunicazioni per fare in modo che il router r5 non venga a conoscenza del loro contenuto.

Comandi per il router r4

Analizziamo il comando da inserire nel router in due parti: nella prima fase introduciamo le impostazioni per effettuare lo scambio delle chiavi e utilizzare il protocollo ISAKMP per identificare l'algoritmo di hashing e il metodo di autenticazione.

◀ The Internet Security Association and Key Management Protocol (ISAKMP) defines procedures and packet formats to establish, negotiate, modify and delete Security Associations (SA). ▶

È anche necessario indicare "la terminazione" del tunnel, che nel nostro caso è sul router r4 di indirizzo 192.168.3.1.

```
crypto isakmp policy 10
hash md5
authentication pre-share // utilizza la chiave di definita in seguito
crypto isakmp key P5NM address 192.168.3.1     //chiave di cifratura
isakmp ccm
```

Procediamo creando IPsec definendo la trasformazione che chiamiamo SEGRETO con l'indicazione del protocollo di crittografia che deve essere diverso da quello utilizzato da IKE.

```
crypto ipsec transform-set SEGRETO esp-3des esp-md5-hmac
mode transport
crypto ipsec df-bit clear
```

Possiamo anche definire un gruppo e richiedere le credenziali per l'utilizzo della VPN.

```
crypto isakmp client configuration group AMICI
key AMICI
```

Settiamo infine la cripto-mappa che verrà utilizza nel sistema.

```
crypto map MIAMAPPA 10 ipsec-isakmp    // definizione di una
set peer 192.168.3.1      // estremo del tunnel
set transform-set SEGRETO       // abilitiamo la trasformazione
match address 101  // origine-destinazione dei pacchetti
crypto map MIAMAPPA       // attiva la cripto map
```

Comandi per il router r3

I comandi per il router r3 sono identici a quelli sopra descritti per il router r4: cambia solamente l'indirizzo di fine tunnel, che è 192.168.2.2.

Prova adesso!

- Programmare i router Cisco in CLI
- Applicare una VPN

Inserisci nei router i comandi sopra descritti e verifica il funzionamento, analizzando i pacchetti che attraversano il router r5.

Esercitazioni di Laboratorio 4

LE ACCESS CONTROL LIST CON PACKET TRACER

Una lista di controllo degli accessi, spesso chiamata col nome inglese di Access Control List (ACL), è un meccanismo usato per esprimere regole complesse che determinano l'accesso ad alcune risorse di un sistema informatico.

Tra le sue applicazioni principali si ha la configurazione di firewall e router e dei diritti di accesso a file e directory da parte del sistema operativo sui propri utenti.

Le ACL vengono realizzate per:
- limitare il traffico in rete;
- fornire controllo del flusso di traffico (es. le ACL possono restringere la consegna degli update di routing);
- offrire un livello base di sicurezza per l'accesso alla rete;
- decidere che tipi di traffico debbano essere instradati o bloccati alle interfacce del router;
- permettere a un amministratore di controllare che un client possa accedere a una rete;
- schermare alcuni host per permettere o negare accesso a parte della rete.

Nelle ACL vengono quindi elencate in ordine le regole che indicano quali utenti o processi di sistema possono accedere a degli oggetti, e quali operazioni sono possibili su particolari oggetti.
Ciascuna regola, definita Access Control Entry (ACE), esprime una o più proprietà dell'oggetto da valutare (sempre in riferimento all'esperienza, l'indirizzo sorgente di un pacchetto IP), e se queste proprietà sono verificate indica quale decisione prendere (es. far passare il pacchetto oppure rifiutarlo).
La valutazione inizia dalla prima regola e continua fino a quando le condizioni di una regola non sono verificate. Se le condizioni sono verificate, la valutazione finisce e viene applicata la decisione presa; altrimenti, la valutazione prosegue alla regola successiva. Se nessuna regola viene soddisfatta, viene applicata una decisione di default, chiamata policy dell'ACL.

Le ACL possono essere usate per controllare il traffico ai livelli 2, 3, 4 e 7: in passato venivano usate le ACL numeriche per filtrare il traffico in base al campo Ethernet Type delle Trame oppure in base agli indirizzi MAC mentre oggi le ACL sono più spesso basate sugli indirizzi IPv4 o IPv6 e sulle Porte TCP e/o UDP.

Le ACL utilizzano un nuovo tipo di maschera, la WildCard Mask.

WildCard Mask

La WildCard Mask è un numero di 32 bit diviso in 4 ottetti. Quest'ultimo conserva la stessa divisione (8 bit per ottetto) della notazione decimale puntata degli indirizzi IPv4. Questa, solitamente, viene abbinata a un indirizzo IP, in modo simile alla SubNet Mask e i bit assumono valori 1 o 0 per stabilire come elaborare i corrispondenti bit dell'indirizzo IP. Il termine stesso indica il procedimento di checking su una qualsiasi Access List, tramite una maschera.

L'analogia nasce dal Jolly (WildCard), usato nel gioco del poker, che permette l'abbinamento, a tale carta, di una qualsiasi altra pari, presente nel mazzo.

Più precisamente, gli 0 e 1 nella WildCard Mask stabiliscono se i bit, corrispondenti nell'indirizzo IP, devono essere controllati o ignorati. Ogni bit a 0, della WildCard Mask, indica che il bit corrisposto dev'essere incluso nel processo di controllo dell'uguaglianza, mentre il valore 1 tralascia ogni vincolo di confronto.

ESEMPIO

Vediamo un esempio per comprendere l'utilizzo della WildCard mask: si supponga di voler effettuare un controllo dell'indirizzo IP: 169.12.5.0/24, che appartiene a una B 169.12.0.0 dove possono essere create 255 reti che contengono 253 host ognuna.

Si desidera bloccare il traffico in arrivo dai seguenti indirizzi IP: da 169.12.5.4 a 170.12.5.7.

169.12.5.0, in binario, è tradotto in 10101010.00001100.00000101.00000000 e la subnet mask è 11 111111.11111111.11111111.00000000 (un /24, come già visto, è un 255.255.255.0).

Guardando gli indirizzi da bloccare in formato binario si osserva che c'è una parte di indirizzo che non cambia:

```
169.12.5.4 - 10101010.00001100.00000101.000001 00
169.12.5.5 - 10101010.00001100.00000101.000001 01
169.12.5.6 - 10101010.00001100.00000101.000001 10
169.12.5.7 - 10101010.00001100.00000101.000001 11
```

Tramite la WildCard Mask, è possibile raggruppare gli indirizzi IP interessati in un'unica dicitura e, come per il CIDR, ridurre il numero di ACL da impostare per bloccare il traffico.
In questo caso è possibile impostare una sola ACL per fermare i dati in arrivo dal range che va dal 169.12.5.4 al 169.12.5.7: è sufficiente individuare l'indirizzo di inizio sequenza che corrisponde all'insieme dei bit non mutevoli:

```
Dot Notation   parte dell'indirizzo non mutevole   parte mutevole
-----------------------------------------------------------------
169.12.5.4 10101010.00001100.00000101.000001 + 00
169.12.5.5 10101010.00001100.00000101.000001 + 01
169.12.5.6 10101010.00001100.00000101.000001 + 10
169.12.5.7 10101010.00001100.00000101.000001 + 11
```

In tutti e quattro gli indirizzi la parte che non cambia è 170.12.5.4 e sarà l'inizio sequenza che ci permette di individuare la WildCard Mask esatta, composta dal valore 1 nella posizione dei bit che mutano, cioè solo gli ultimi 2:
la WildCard Mask, in forma binaria, sarà `00000000.00000000.00000000.00000011`.
In forma decimale puntata `0.0.0.3`.

Scrivere le ACL

Prima di scrivere le ACL è necessario aggiungere il comando che indica se il gruppo di dispositivi/servizi relativo all'ACL è da riferirsi alle richieste in entrata (in e inbound) oppure in uscita (out e outbound).

Definire In, Out, Inbound, Outbound

Vediamo le differenze tra le diverse situazioni:

- out: si riferisce al traffico che ha attraversato il router e lascia l'interfaccia;
- in: è il traffico che arriva sulla interfaccia e poi passa attraverso il router;
- inbound: se la lista di accesso è in entrata, quando il router riceve un pacchetto, il software Cisco IOS controlla i criteri della ACL e se al pacchetto è consentito l'accesso continua a elaborarlo altrimenti lo scarta;
- outbound: se la lista di accesso è in uscita, quando il software riceve l'indirizzo dell'interfaccia d'uscita, controlla i criteri della ACL e se è consentito a quel pacchetto di raggiungere l'interfaccia, lo trasmette, altrimenti lo scarta.

◀ The out ACL has a source on a segment of any interface other than the interface to which it is applied and a destination off of the interface to which it is applied.
The in ACL has a source on a segment of the interface to which it is applied and a destination off of any other interface. ▶

Quindi per applicare le ACL alle interfacce e alle linee VTY, in ingresso o in uscita dal router, si utilizzano i seguenti comandi:

```
R(config-if)#ip access-group numero {in | out}      // per le interfacce
R(config-line)#access-class numero {in | out}       // per le linee VTY
```

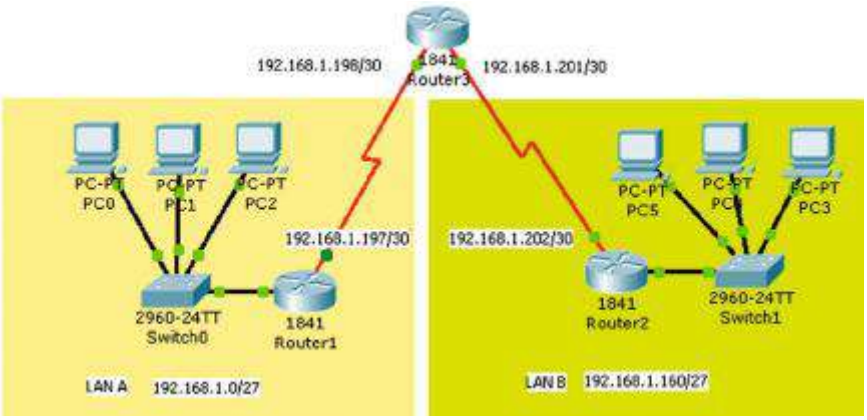
ACL Standard

Le ACL Standard numeriche per IPv4 e IPv6 hanno numero da 1 a 99 e da 1300 a 1999; esse controllano solo l'IP sorgente dei Pacchetti, e non possono indicare alcun protocollo L4-L7:

```
R(config)#access-list numero {permit | deny} IP-sorgente [wildcard mask]
```

ESEMPIO

Consideriamo la rete di figura, è richiesto di scrivere la ACL affinché i PC della LAN A non possano accedere alla LAN B.



I comandi sono i seguenti:

```
Router2(config)#access-list 10 deny 192.168.1.0 0.0.0.31 //wildcard 0.0.0.00011111
Router2(config)#access-list 10 permit any
```

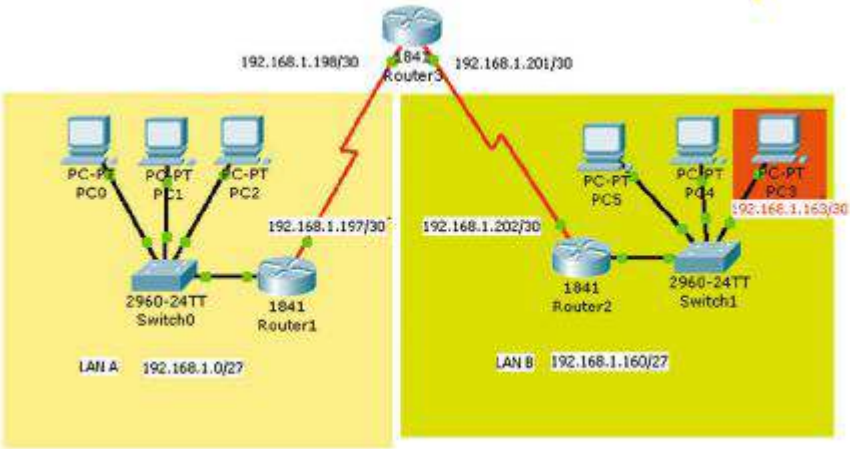
(Il file con memorizzata la rete è 1.St ACL con network deny.pkt).

Prova adesso!

- Programmare i router Cisco in CLI
- Applicare le ACL

Realizza la rete mostrata in figura a pagina precedente e verifica il funzionamento prima dell'inserimento della ACL. Quindi inserisci nel router2 la ACL sia manualmente attraverso l'interfaccia CLI che modificando il file di configurazione Running Config aggiungendo le righe come sotto indicato:

Se invece vogliamo vietare l'accesso di un solo computer, per esempio il PC3 di indirizzo IP 192.168.1.163 indicato nella figura:



i comandi sono i seguenti:

```
Router1(config)#access-list 10 deny host 192.168.1.163
Router1(config)#access-list 10 permit any
```

(Il file con memorizzata la rete è 2.St ACL con PC deny.pkt).

Prova adesso!

- Programmare i router Cisco in CLI
- Applicare le ACL

Realizza la rete mostrata in figura a pagina 231 e verifica il funzionamento prima dell'inserimento della ACL. Quindi inserisci nel router1 la ACL sia manualmente attraverso l'interfaccia CLI che modificando il file di configurazione Running Config aggiungendo le righe come sotto indicato:

Quindi modifica le ACL dei due router in modo che i router con indirizzo pari possano raggiungere tutti gli altri host mentre quelli di indirizzo dispari possano raggiungere solo gli host della propria sottorete.

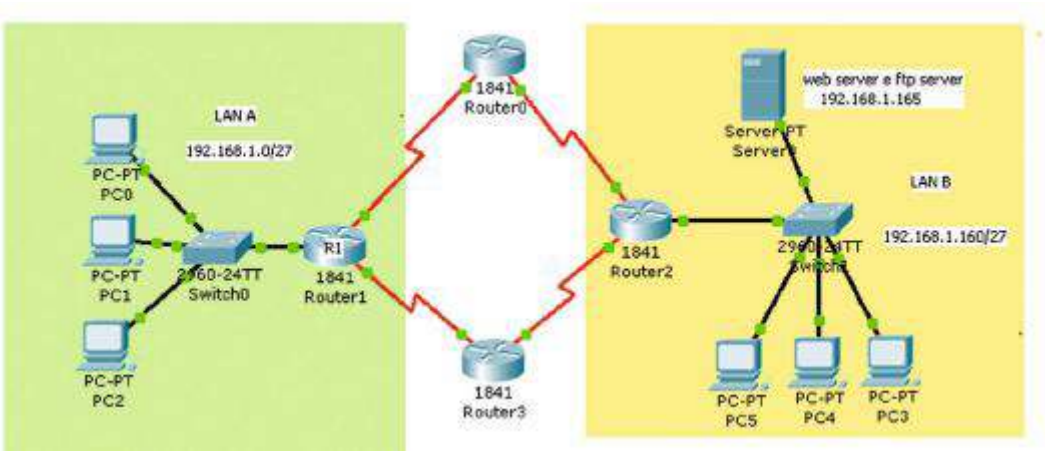
ACL Estese

Le ACL Estese numeriche per IPv4 e IPv6 hanno numero da 100 a 199 e da 2000 a 2699; esse controllano i Pacchetti in base sia all'IP sorgente sia alla destinazione, e possono anche indicare un protocollo L4 (TCP o UDP) e L7 (Porte Well-known).
La sintassi (semplificata) del comando è:

```
R(config)#access-list numero {permit | deny} protocollo
IP-sorgente wildcard mask [operator Port [Port]]
IP-destinaz wildcard mask [operator Port [Port]] [established]
```

ESEMPIO

Nella rete seguente si vuole inibire alla LAN A di utilizzare il Web server e il servizio FTP offerto sempre dallo stesso server 192.168.1.165.



I comandi per la configurazione del router 1 sono i seguenti:

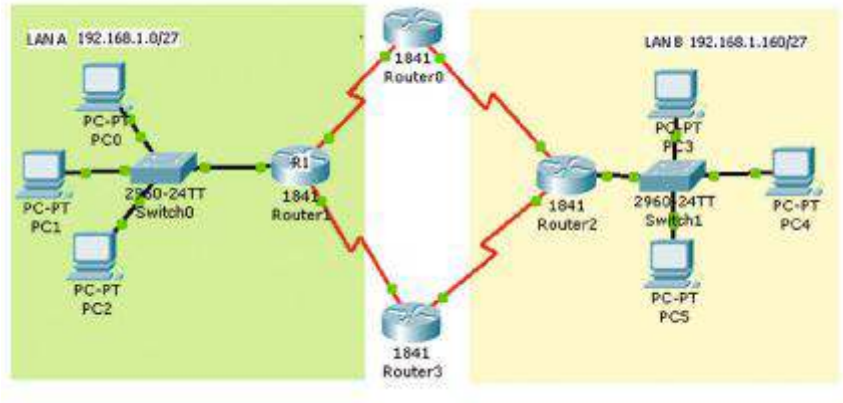
Ricordiamo di aggiungere il comando per la configurazione della interfaccia:

```
R1(config-if)#ip access-group 100 in
```

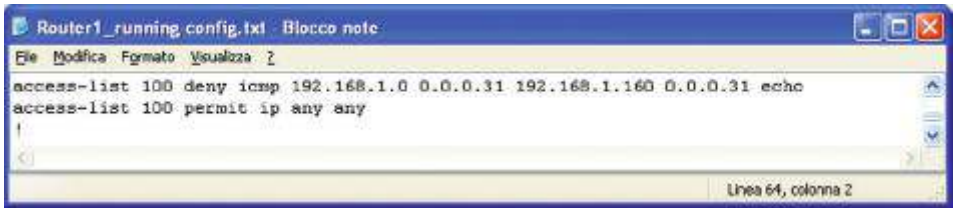
(Il file con memorizzata la rete è 3.Ext ACL con limitazione servizi.pkt).

ESEMPIO

Vediamo un secondo esempio dove la LAN A non può accedere a LAN B ma LAN B può accedere a LAN A utilizzando ICMP.



I comandi per la configurazione del router 1 sono i seguenti:



ricordiamo di aggiungere il comando per la configurazione della interfaccia:

```
R1(config-if)#ip access-group 100 in
```

(Il file con memorizzata la rete è 3.Ext ACL con limitazione servizi.pkt).

Concludiamo con due osservazioni.

1. Le ACL, sia standard sia estese, hanno un deny finale implicito; se devono consentire il traffico diverso da quello specificato, inserire un permit finale esplicito.
2. Le ACL possono anche avere un nome invece di un numero; vengono create col comando:

```
R(config)#ip access-list {standard | extended} nome-ACL
```

Le "entry" di una ACL con nome possono essere cancellate, aggiunte anche in posizione intermedia o modificate singolarmente, a differenza delle ACL numeriche che si possono solo riscrivere tutte.

Zoom su...

ROUTER E ACL

Descriviamo la sequenza delle operazioni che vengono eseguite da un router nell'analisi di un pacchetto:

1. non appena una PDU di strato 2 entra in un'interfaccia, il router verifica l'indirizzo di strato 2 se corrisponde al suo indirizzo o è un indirizzo di broadcast;
2. se il check è positivo, il router estrae allora il pacchetto ed esamina la ACL associata all'*interfaccia di ingresso*, sempre che ne sia definita una;
3. il router esegue ogni comando della ACL;
4. se si riscontra una corrispondenza sulla condizione corrispondente a un comando, il router compie l'azione collegata a quel comando;
5. se il pacchetto è accettato il router eseguirà la funzione di instradamento;
6. se è definita una ACL sull'*interfaccia di uscita*, il pacchetto sarà di nuovo testato in base ai comandi contenuti in questa ACL;
7. se tutti i test autorizzano il pacchetto a proseguire il suo cammino, questo viene incapsulato nel protocollo di strato 2 definito sull'interfaccia d'uscita.

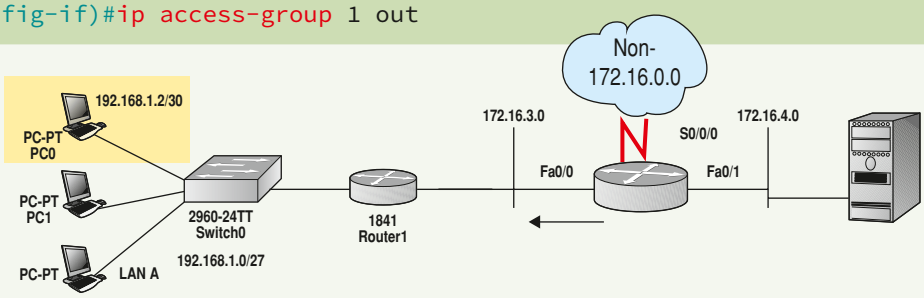
Prova adesso!

- Programmare i router Cisco in CLI
- Applicare le ACL

Nella rete seguente.

1. Configura il router in modo tale che la subnet 172.16.4.0 non debba accedere solo alla subnet 172.16.3.0 utilizzando una ACL1 per l'interfaccia di uscita:

```
R1(config)#access-list 1 deny 172.16.4.0 0.0.0.255
R1(config)#access-list 1 permit any
R1(config)#interface fa0/0
R1(config-if)#ip access-group 1 out
```



2 Vieta il traffico FTP tra le due subnet utilizzando una ACL2 estesa:

```
R1(config)#access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
;21 = Porta comandi dell'FTP
R1(config)#access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20
R1(config)#access-list 101 permit ip any any
R1(config)#interface fa0/1
R1(config-if)#ip access-group 101 in          ;evita traffico nel Router
```

3 Progetta ora due nuove ACL affinché vengano rispettati i seguenti vincoli:

ACL3: restringe l'accesso alle linee VTY in modo che non venga inoltrato il traffico proveniente da tutti gli indirizzi del tipo 192.168.Z.90 (per ogni Z≠X);

ACL4: restringe l'accesso alle interfacce d'ingresso del router in modo che venga inoltrato il traffico diretto verso l'host PC0 e il traffico ICMP diretto verso le interfacce del router.

4 Verifica la correttezza dell'ACL definita con il comando RouterX# show access-list e mediante i comandi PING e TRACEROUTE.

5 Salva il file di configurazione attuale in quello di startup.

```
RouterX# copy run start.
```

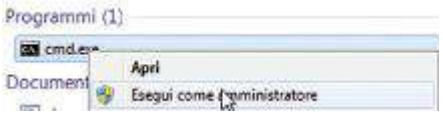
Esercitazioni di Laboratorio 5

CERTIFICATI DIGITALI CON APACHE

Certificato digitale

Vediamo come realizzare un certificato digitale che venga utilizzato dal server Apache, in esecuzione sotto XAMPP, per realizzare la connessione sicura in HTTPS.

1. Digitiamo cmd.exe dal menu Esegui di Windows, quindi tasto destro del mouse e Esegui come amministratore per aprire il prompt dei comandi. ▶



2. Posizioniamoci nella directory C:\xampp\apache\bin del disco fisso, con il comando seguente:

```
cd c:\ xampp\apache\bin.
```

3. A questo punto configuriamo le variabili d'ambiente necessarie per attivare il protocollo SSL con i comandi seguenti:

```
set OPENSSL_CONF=G:\xampp\apache\conf\openssl.cnf
set RANDFILE=C:\Windows\Temp\.rnd
```

4. A questo punto possiamo creare il certificato con firma digitale attraverso il comando openssl che apre l'ambiente operativo OpenSSL:

```
C:\Windows\system32>cd c:\xampp\apache\bin

c:\xampp\apache\bin>set OPENSSL_CONF=C:\xampp\apache\conf\openssl.cnf

c:\xampp\apache\bin>set RANDFILE=C:\Windows\Temp\.rnd

c:\xampp\apache\bin>openssl
OpenSSL>
```

5. Eseguiamo il comando seguente per creare una chiave criptata a 1024 bit:

```
genrsa -des3 -out server.key 1024
```

Al termine dell'esecuzione del comando ci viene richiesto l'inserimento della password, che viene richiesta due volte, come mostrato nella figura sottostante:

```
OpenSSL> genrsa -des3 -out server.key 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.++++++
.....................................++++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
OpenSSL>
```

Possiamo anche fare una copia della chiave per evitare di dover riscrivere la password ogni volta. Per fare questo usciamo da OpenSSL con exit, quindi digitiamo il comando seguente:

```
copy server.key server.key.org
```

La copia genera una chiave in uscita, dopo esserci di nuovo posizionati nell'ambiente OpenSSL (comando `openssl`), diamo il comando seguente:

```
rsa -in server.key.org -out server.key
```

6 Vediamo infine come creare effettivamente il certificato digitale, per fare questo digitiamo il comando seguente:

```
req -new -x509 -nodes -sha1 -days 365 -key server.key -out server.crt
-config C:\xampp\apache\bin\openssl.cnf
```

Come possiamo notare vengono richiesti alcuni parametri: `Country Name`, `Organization Name` ecc. Possiamo premere Invio senza inserire alcun valore, l'unico parametro che deve essere inserito è `Common Name`, che rappresenta il dominio: digitiamo quindi `localhost`:

```
OpenSSL> req -new -x509 -nodes -sha1 -days 365 -key server.key -out server.crt
-config C:\xampp\apache\bin\openssl.cnf
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:localhost
```

7 Come possiamo notare sono stati creati i file server.key e server.crt all'interno della directory c:\xampp\apache\bin:

Affinché la creazione del certificato necessario all'esecuzione del protocollo HTTPS sia completata dobbiamo copiare i file server.key e server.crt nelle sottodirectory ssl.crt e ssl.key della directory c:\xampp\apache\conf.

8 Dobbiamo quindi abilitare le istruzioni seguenti nel file httpd.conf, presente nella directory c:\xampp\apache\conf, togliendo il cancelletto (simbolo di commento `#`) posto all'inizio della riga e salvando poi le modifiche:

```
#LoadModule ssl_module modules/mod_ssl.so
#include conf/extra/httpd-ssl.conf
```

9 Apriamo il file php.ini, presente nella directory c:\xampp\php, togliendo il punto e virgola (simbolo di commento `;`) posto all'inizio della riga e salvando poi le modifiche:

```
;extension=php_openssl.dll
```

10 Apriamo il file `httpd_ssl.conf`, presente nella directory `c:\xampp\apache\conf\extra`, quindi verifichiamo che le righe seguenti non siano commentate:

```
SSLCertificateFile "conf/ssl.crt/server.crt"
SSLCertificateKeyFile "conf/ssl.key/server.key"
```

11 Verifichiamo infine il certificato, eseguendo il comando seguente:

```
httpd -t
```

Se appare il risultato `Syntax OK`, significa che il codice non ha errori:

```
c:\xampp\apache\bin>httpd -t
Syntax OK
```

Prova adesso!

- Applicare i certificati digitali al Web server Apache

Dopo aver installato il certificato, come mostrato nella lezione, verifica il funzionamento aprendo con il browser la pagina di apertura del server XAMPP:
`https://localhost`

CLIL

G8 officials and the private sector meet to discuss combating computer crime
Senior representatives of the governments and the private sector from all G8 countries, and the European Commission, met in Tokyo from 22 to 24 May, 2001, to continue discussions on combating high-tech crime and the criminal exploitation of the Internet by exploring possible solutions that enhance the public interest, including the protection of public safety, privacy and other social values and the encouragement of the growth of the information society and e-commerce.

Code red
The original Code Red worm initiated a distributed denial of service (DDoS) attack on the White House. That means all the computers infected with Code Red tried to contact the Web servers at the White House at the same time, overloading the machines. "Code Red Worm", also known as I-Worm.Bady and W32/Bady.worm from Symantec Antivirus Research Center, is a self-replicating malicious code that exploits a known vulnerability in IIS servers. Once it has infected a system, it multiplies itself and it begins scanning random IP addresses at TCP port 80 looking for other IIS servers to infect.

Worm
A worm is a destructive program that replicates itself throughout a single computer or across a network, both wired and wireless. It can do damage by sheer reproduction, consuming internal disk and memory resources within a single computer or by exhausting network bandwidth. It can also deposit a Trojan that turns a computer into a zombie for spam and other malicious purposes. Very often, the terms "worm" and "virus" are used synonymously; however, worm implies an automatic method for reproducing itself in other computers.

Attacks
"Attack technology is developing in a open-source environment and is evolving rapidly."

"Defensive strategies are reactionary."

"Thousands – perhaps millions – of systems with weak security are connected to the Internet."

"The explosion in use of the Internet is straining our scarce technical talent. The average level of system administrators [...] has decreased dramatically in the last 5 years."

"Attacks and attack tools transcend geography and national boundaries."

"Increasingly complex software is being written by programmers who have no training in writing secure code."

"The difficulty of criminal investigation of cybercrime coupled with the complexity of international law means that […] prosecution of computer crime is unlikely."

X.509
A widely used standard for defining digital certificates, X.509 (Version 1) was first issued in 1988 as a part of the ITU X.500 Directory Services standard. When X.509 was revised in 1993, two more fields were added, resulting in the Version 2 format. These two additional fields support directory access control. X.509 Version 3 defines the format for certificate extensions used to store additional information regarding the certificate holder and to define certificate usage. Collectively, the term X.509 refers to the latest published version, unless the version number is stated.

Spam
Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Most spam is commercial advertising, often for dubious products, get rich quick schemes, or quasi-legal services. Spam costs the sender very little to send: most of the costs are paid for by the recipient or the carriers rather than by the sender.

Self-signed Certificated
A self signed certificate is a certificate that is signed by itself rather than a trusted third party. This means you can't verify that you are connecting to the right server because any attacker can create a self signed certificate and launch a man-in-the-middle attack. Because of this, you should almost never use a self signed certificate on a public server that requires anonymous visitors to connect to your site.

Cipher suite
A cipher suite is a collection of security algorithms that determine precisely how an SSL/TLS connection is implemented: the SSL/TLS protocol mandates that messages be signed using a message digest algorithm. The choice of digest algorithm, however, is determined by the particular cipher suite being used for the connection (MD5 or the SHA digest algorithm).

Filtering router
A router which examines packets of data and filters those packets which a system administrator has determined should not reach certain destinations. A good example of the use of a filtering router is in implementing a firewall using a proxy server.

DMZ (DeMilitarized Zone)
A middle ground between an organization's trusted internal network and an untrusted, external network such as the Internet. Also called a "perimeter network", the DMZ is a subnetwork (subnet) that may sit between firewalls or off one leg of a firewall. Organizations typically place their Web, mail and authentication servers in the DMZ. DMZ is a military term that refers to the area between two enemies.

UNITÀ DI APPRENDIMENTO

5

Wireless e reti mobili

L1 **Wireless: comunicare senza fili**
L2 **L'autenticazione nelle reti wireless**
L3 **La trasmissione wireless**
L4 **L'architettura delle reti wireless**
L5 **La normativa delle reti wireless**

Esercitazioni di laboratorio

1 Access Poi8t Li8ksys co8 Packet T=ace=; 2 Se=ve=Radius co8 Packet T=ace=; 3 Co8t=olla=e gli accessi wi=eless co8 Wi=eless Netwo=k Watche=

Conoscenze

- Conoscere i compo8e8ti di u8a =ete wi=eless
- App=e8de=e le topologie e gli sta8da=d di comu8icazio8e wi=eless
- Co8osce=e le modalità di sicu=ezza co8 c=ittog=afia WEP
- Co8osce=e le modalità di sicu=ezza WPA e WPA2
- Comp=e8de=e il sistema di aute8ticazio8e 802:1X
- Co8osce=e il p=otocollo EAP
- A8alizza=e il fo=mato del f=ame 802.11
- Co8osce=e la 8o=mativa sulle emissio8i elett=omag8etiche
- Co8osce=e la 8o=mativa sugli accessi wi=eless pubblici

Competenze

- Co88ette=e u8 Access Poi8t Li8ksys a u8a =ete LAN
- A8alizza=e il t=affico wi=eless
- Aute8tica=e dispositivi wi=eless co8 se=ve=Radius
- Utilizza=e sistemi di p=otezio8e WPA2 PSK e WPA2 TKIP

Abilità

- A8alizza=e il livello fisico e la t=asmissio8e dei seg8ali wi=eless
- Sape=defi8i=e le topologie delle =eti wi=eless
- Co8osce=e gli sta8da=d di comu8icazio8e wi=eless
- Sceglie=e le politiche di sicu=ezza pe=u8a =ete wi=eless
- I8dividua=e i dispositivi co88essi a u8a =ete wi=eless
- I8dividua=e i possibili attacchi alla sicu=ezza di u8a =ete wi=eless

AREA digitale

Esercizi

Soluzioni
Puoi scaricare il file anche da hoepliscuola.it

LEZIONE 1

Wireless: comunicare senza fili

In questa lezione impareremo...

- i componenti di una rete wireless
- le topologie e gli standard di comunicazione wireless

Topologia

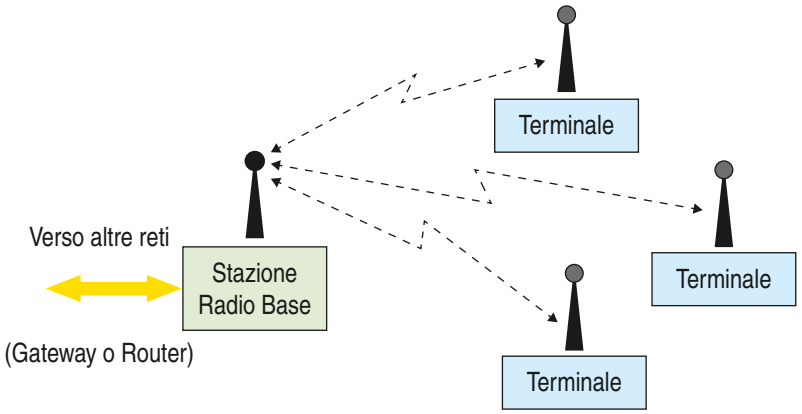
Tra le reti wireless, cioè tutte le reti in cui i terminali accedono alla rete tramite canali "senza fili" (in genere onde radio), possiamo distinguere due famiglie:

A reti radiomobili sono reti wireless dove i terminali utenti possono spostarsi sul territorio senza perdere la connettività con la rete, come la rete cellulare;

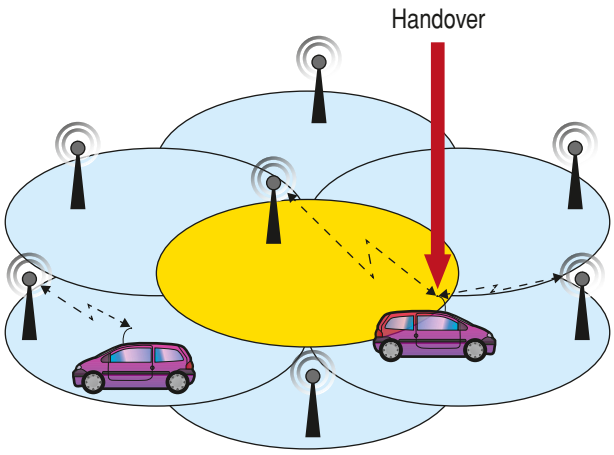
B Wireless LAN (WLAN) sono reti wireless che forniscono coperture e servizi tipici di una LAN.

Dobbiamo sottolineare una differenza fondamentale tra reti wireless e reti cellulari:

- rete wireless: è una (sotto) rete in cui l'accesso da un terminale avviene attraverso un canale "senza filo";



- rete cellulare: è una rete la cui copertura geografica è ottenuta con una tassellatura di aree adiacenti e/o sovrapposte, dette celle, dove l'utente si può muovere attraverso la rete passando da una cella all'altra, senza interrompere la comunicazione.



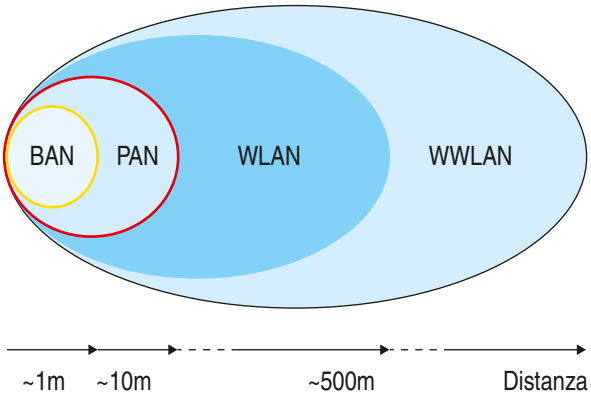
Anche se in entrambe i dispositivi che sono connessi sono mobili, nel primo l'accesso alla rete è generalmente unico (stazione radio base o Access Point) e il terminale mobile si sposta "all'interno della stessa rete" mentre nelle reti cellulari la connessione deve essere "passata" tra celle adiacenti senza che venga a perdersi il collegamento: questo passaggio prende il nome handover (o handoff) e, di fatto, è l'elemento distintivo tra le reti cellulari e ogni altro tipo di rete TLC.

> Le procedure connesse agli handover sono complesse e richiedono alle reti notevoli requisiti in termini di architettura di rete, di protocolli e di segnalazione.

Le funzionalità aggiuntive che devono essere svolte in sistemi che presentano utenti in "mobilità" sono sostanzialmente:

- localizzazione: ogni utente mobile deve essere localizzato nell'area di copertura individuando la sua posizione;
- registrazione: un terminale mobile, dopo che viene localizzato, deve venire "collegato" alla rete e quindi deve venire identificato e autenticato;
- handover: al passaggio tra due zone avviene la (ri)localizzazione e, quindi, la sua (ri)registrazione.

Come per le reti cablate anche per le reti wireless viene fatta una classificazione sulla base della distanza geografica che il segnale trasmesso dai dispositivi che si connettono alla rete può raggiungere, cioè "l'area di copertura"; definiamo quattro categorie di reti.



BAN (Body Area Network)

Con Body Area Network si intendono le reti wearable, cioè o indossabili o nelle immediate vicinanze del corpo, con un raggio di copertura al massimo di due metri: i dispositivi coinvolti sono i telefoni cellulari, gli auricolari, i palmari, i lettori Mp3 ecc.
Proprio per l'utilizzo sul corpo questi dispositivi devono essere connessi tra loro senza fili e, generalmente, hanno la capacità di autoconfigurarsi anche se sono di tipo diverso.

PAN (Personal Area Network)

Le Personal Area Network sono reti con area di copertura che raggiunge anche i dieci metri, generalmente all'interno di un locale: è ad esempio la rete personale dell'ufficio dell'utente, dove i dispositivi mobili si connettono con quelli fissi, computer e/o stampanti per condividere informazioni e risorse.
I moderni sistemi operativi offrono delle applicazioni predisposte alla sincronizzazione automatica dei dispositivi mobili con quelli fissi che nella PAN generalmente si connettono con tecnologie a infrarossi o radio: le macchine digitali ad esempio scaricano le fotografie sui desktop, il lettore mp3 riceve nuove canzoni appena scaricate da Internet ecc.
Per la sua sicurezza ed economicità lo standard Bluetooth è di fatto quello prevalentemente usato per scambiare informazioni tra dispositivi diversi attraverso una frequenza radio a corto raggio: sfrutta onde nello spettro dell'infrarosso nelle frequenze libere di 2,45 GHz con una bit rate di 3 Mbps.
Le specifiche per il Bluetooth rientrano nello standard IEEE 802.15.

WLAN (Wireless Local Area Network)

Le WLAN sono le reti maggiormente diffuse con il loro raggio di copertura che va dai 100 ai 500 metri: possono quindi raggiungere i dispositivi all'interno di un edificio di medie dimensioni, come una scuola o una piccola impresa, e possono sostituire a tutti gli effetti le LAN cablate offrendo le stesse prestazioni e possibilità di connettività.
Una rete WLAN è costituita da ◀ Station (STA) ▶ e Access Point (AP).

◀ Con Station si indica un dispositivo che contiene interfacce MAC e PHY wireless conformi allo standard IEEE 802.11, ma non fornisce accesso al sistema di distribuzione (terminali tipo work station, laptop ecc.). Le STA sono anche indicate come Wireless Terminal WT e sono dotate di una interfaccia 802.11 integrata oppure su schede USB o PCMCIA, e possono essere sia terminali mobili che fissi (palmari, netbook, smartphone ecc.). ▶

Con Access-Point si indica un dispositivo che contiene interfacce wireless MAC e PHY conformi allo standard IEEE 802.11, che consente l'accesso a un sistema di distribuzione per le stazioni associate: solitamente sono elementi di infrastruttura che sono connessi a backbone cablati.

Le Wireless LAN sono regolate dallo standard IEEE 802.11: dalla 802.11b in poi sono anche chiamate semplicemente Wi-Fi (wireless fidelity), marchio definito da un consorzio di imprese che ormai è divenuto sinonimo di wireless.

Il termine 802.11 viene usualmente utilizzato per definire la prima serie di apparecchiature 802.11 sebbene si debba preferire il termine "802.11 legacy".

Troviamo nelle WLAN gli stessi requisiti delle tradizionali reti LAN cablate (wired), come la completa connessione fra le stazioni che ne fanno parte e la capacità di inviare messaggi broadcast.
I problemi con questa tipologia di rete sono quelli classici delle connessioni wireless, e cioè la sicurezza delle informazioni, la larghezza di banda limitata e il consumo energetico.

WWAN (Wireless Wide Area Network)

Le WWAN sono reti wireless di dimensione geografica estesa sino a una decina di kilometri e nascono dall'esigenza di raggiungere utenti che difficilmente potrebbero avere connessioni cablate, come paesi di montagna o aree difficilmente raggiungibili e/o antieconomiche per le normali linee fisse.
Le soluzioni WWAN che si basano su un'infrastruttura a rete cellulare, o su trasmissione satellitare, rappresentano il futuro della comunicazione dati, permettendo a chiunque di accedere ai dati e scambiare informazioni.

Le reti WWAN sono realizzate con diversi standard: ricordiamo le generazioni che hanno caratterizzato la loro evoluzione:

- prima generazione (1G): nato negli Stati Uniti, lo standard Advanced Mobile Phone Systems (AMPS) permetteva la trasmissione della voce tra cellulari Tacs in tecnologie analogiche su una banda di frequenza di 800 MHz;
- seconda generazione (2G): si basavano su tecnologia digitale per servizi telefonici, come il Global System for Mobile (GSM) in Europa e Personal Digital Communication (PDC) in Giappone, con data rate prevista che non superava 9.6 Kbps;
- seconda generazione e mezzo (2.5G): è l'evoluzione della precedente e con il General Packet Radio System (GPRS) e EDGE oltre alla voce iniziò a effettuare la trasmissione dei dati (data rate di 348 Kbps);
- terza generazione (3G): con l'Universal Mobile Telecommunication System (UMTS) si raggiungono trasmissioni con data rate fino a 2 Mbps su frequenze di trasmissione comprese fra 1, 9 GHz e i 2, 2 GHz e si rendono disponibili nuovi servizi quali videotelefonate e trasferimento di filmati.

Analogamente a quanto successo con Wi-FI è nato WiMAX, un consorzio di imprese dedicate a progettare i parametri e gli standard per questa tecnologia che consente l'accesso a reti di telecomunicazioni a banda larga e senza fili.

L'acronimo è stato definito in occasione del WiMAX Forum al quale hanno partecipato più di 420 aziende riunite allo scopo di collaborare per produrre dispositivi compatibili e testare l'interoperabilità di sistemi basati sullo standard IEEE 802.16, conosciuto anche come WirelessMAN (Wireless Metropolitan Area Network).
Il WiMAX consente oggi agli utenti di usufruire di una connessione a larga banda con elevata qualità del servizio, in grado di raggiungere velocità fino a 7 megabit al secondo. Inoltre, utilizzando frequenze concesse in licenza dal Ministero delle Comunicazioni e implementando tecniche di crittografia e autenticazione contro intrusione di terzi, assicura un notevole grado di affidabilità ed elevati standard di sicurezza.

Lo standard IEEE 802.11

Prima di analizzare le caratteristiche delle reti WLAN è necessario effettuare una panoramica dei protocolli della famiglia dello standard IEEE 802.11 per le WLAN e le specifiche Bluetooth per le comunicazioni wireless a corto raggio.

Il protocollo 802.11 legacy

Il gruppo IEEE 802.11 è stato costituito nel 1989 e ha sviluppato diverse classi di reti: nel 1997 ha divulgato il primo standard di riferimento per le reti wireless, l'IEEE 802.11 legacy, che detta le specifiche a livello "Fisico" (*Physical layer*) e di "Collegamento" (*Data Link layer*) per l'implementazione di una rete LAN wireless:

- velocità di trasferimento dei dati compresa tra 1 e 2 Mbps;
- mezzo trasmissivo: raggi infrarossi nella frequenza di 2,4 GHz per la trasmissione del segnale.

L'uso dei raggi infrarossi venne successivamente abbandonato preferendo la trasmissione radio che meglio si adatta alle esigenze di una rete LAN.

In Europa la banda disponibile per il 802.11 è suddivisa in 13 canali: la frequenza centrale di ciascun canale è riportata nella tabella seguente dove si può vedere che dista dalla più vicina per 5 MHz.

Canale	Frequenze
1	2412 MHz
2	2417 MHz
3	2422 MHz
4	2427 MHz
5	2432 MHz
6	2437 MHz
7	2442 MHz
8	2447 MHz
9	2452 MHz
10	2457 MHz
11	2462 MHz
12	2467 MHz
13	2472 MHz

Le velocità supportate dallo standard sono riportate in tabella correlate con la distanza.

Campo	11 Mbs	5,5 Mbs	2 Mbs	1 Mbs
Ambiente aperto	160 m	270 m	400 m	550 m
Ambiente semi-aperto	50 m	70 m	90 m	115 m
Ambiente chiuso	25 m	35 m	40 m	50 m

802.11 b

Questo standard nato nel 1999 diventa il nuovo standard dominante con il nome di Wi-Fi Wireless Fidelity: viene progettato per un data rate massimo di 11 Mbps utilizzando il metodo CSMA/CA per la trasmissione delle informazioni. Il massimo valore di trasferimento ottenibile è di 5,9 Mbps utilizzando il protocollo TCP e 7,1 Mbps con UDP sfruttando le frequenze nell'intorno dei 2.4 GHz.

802.11 a

Nel 2001 viene ratificato il protocollo 802.11a che utilizza lo spazio di frequenze nell'intorno dei 5 GHz operando con una velocità massima teorica di 54 Mbps: nella pratica raggiunge solamente i 20 Mbps. Lo standard definisce 12 canali non sovrapposti, 8 dedicati alle comunicazioni interne e 4 per le connessioni punto a punto.

802.11 f

Chiamato IAPP (Inter Access Point Protocol), l'802.11f è un protocollo di livello "Applicazione» per la gestione di ESS (Extend Service Set): si occupa di gestire l'handover di terminali da una rete wireless all'altra.

802.11 g

Questo standard viene approvato nel giugno del 2003 e utilizza la stessa frequenza dell'802.11b, ovvero 2,4 GHz. Fornisce una banda teorica di 54 Mbps, che in pratica si traduce a 24.7 Mbps molto simile a quella dell'802.11a; esistono delle varianti proprietarie chiamate g+ o SuperG che utilizzano l'accoppiamento di due canali per raddoppiare la banda disponibile introducendo, però, notevoli interferenze con altre reti.

802.11 i

Lo scopo del progetto 802.11.i è quello di sopperire alle debolezze del sistema crittografico WEP creando una valida alternativa alla crittografia e aumentando la sicurezza generale delle reti wireless.
I risultati ottenuti sono stati ratificati come standard e si dividono in due parti:

1. specifiche crittografiche per l'uso di AES (Advanced Encryption Standard);
2. IEEE 802.1X Port Based Network Authentication Standard: autenticazione e gestione delle chiavi nelle WLAN.

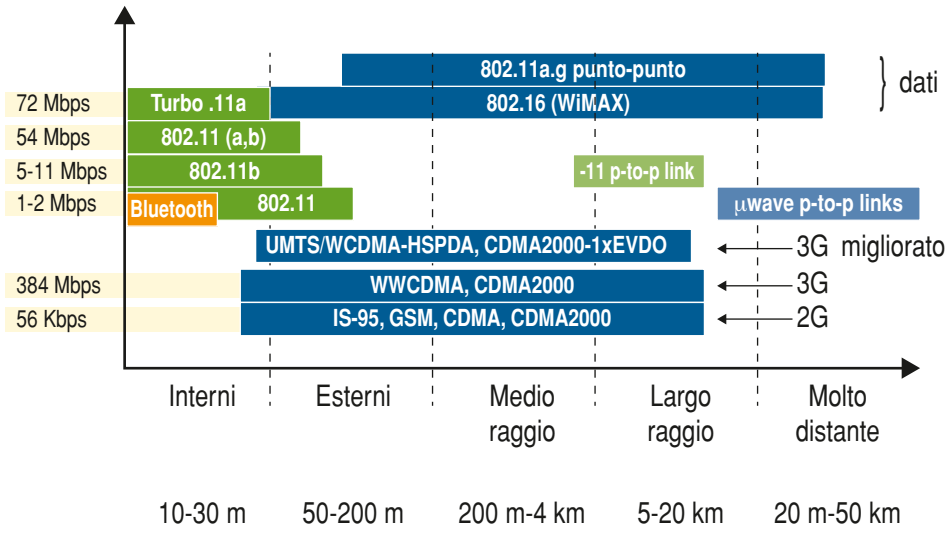
802.11 n

Dal gennaio 2004 l'IEEE attiva un gruppo di studio per realizzare uno standard per le reti wireless di dimensioni metropolitane che dovrebbe supportare una velocità di trasmissione teorica di 250 Mbps (100 Mbps reale) dimostrandosi 5 volte più rapido dell'802.11g e 40 volte più dell'802.11b.

> Una delle caratteristiche innovative del protocollo prevede la possibilità di utilizzare la tecnologia MIMO (Multiple Input Multiple Output) che consente di utilizzare più antenne per trasmettere e ricevere, ampliando la banda disponibile attraverso una multiplazione spaziale.

802.11ac

Avviato da IEEE nel settembre 2008 questo standard dell'802.11 è correntemente in fase di sviluppo e opera nell'intorno delle frequenze dei 5 GHz. La velocità massima teorica di questo standard all'interno di una WLAN multi-stazione è di 1 Gbit/s con una velocità massima di un singolo collegamento di 500 Mbit/s. Ciò è ottenuto ampliando concetti utilizzati da 802.11n: una più ampia larghezza di banda (fino a 160 MHz), più flussi spaziali MIMO (fino a 8), MIMO multi-utente e modulazione ad alta densità (fino a 256 QAM).
La seguente tabella riporta in ascissa la distanza e in ordinata la frequenza di trasmissione dei diversi standard sino a ora descritti.



Altre tecnologie wireless

HiperLAN (HIgh PErformance Radio LAN), standard per comunicazione wireless WLAN che, utilizza una frequenza di 5,4 GHz con bit rate sino a 54 Mbps. Lo standard HiperLAN è derivato dallo standard IEEE 802.11a, con due meccanismi addizionali:

- TCP (Transmitter Power Control) è la capacità dell'apparato HiperLAN di modificare istantaneamente la sua potenza di trasmissione, gli apparati utilizzano solo la potenza necessaria a portare a buon fine la trasmissione in base ad esempio alla distanza.
- DFS (Dynamic Frequency Selection) è la capacità dell'apparato HiperLAN di modificare in modo istantaneo la frequenza di trasmissione, permette all'unità Master di evitare di disturbare i RADAR per la navigazione aerea, comunicando all'unità Slave la nuova frequenza di trasmissione. Infatti le frequenze utilizzate dall'HiperLAN sono le stesse utilizzate dai radar.

IrDA (Infrared Device Application), tecnologia di interconnessione dati che utilizza i raggi infrarossi. È bidirezionale e point-to-point, può avvenire solo tra dispositivi visibili reciprocamente (LoS, line of sight). La distanza è di 2 m e il bit rate è di 4 Mbps.

HomeRF, standard per la trasmissione dati in radio frequenza che utilizza il protocollo Swap. In genere usato per dispositivi domestici, ha una frequenza di lavoro tipica di 2,4 GHz e un bit rate pari a 1,6 Mbps. La versione 2.0 permette un bit rate fino a 10 Mbps e la trasmissione dati/voce con una distanza di 50 m, sia in modalità peer-to-peer che Access Point.

DECT (Digital Enhanced Cordless Telecommunications), standard digitale criptato per telefonini cordless che consente di avere 120 canali su 12 frequenze. Si tratta di una evoluzione del cordless analogico, implementa l'interfaccia Gap (Generic Access Profile) e utilizza la modulazione GMSK, bit rate max 348 Kbps.

WIpLL (Wireless Ip Local loop), tecnologia wireless che fornisce servizi sia voce che dati con copertura ad ampio raggio, utilizzando una frequenza che va da 2 GHz a 5 GHz con un bit rate di 4 Mbps.

Una tipica antenna Hiperlan

Verifichiamo le conoscenze

1. Completamento

1 Le procedure connesse agli handover sono complesse e richiedono alle reti notevoli requisiti in termini di ....., di ..... e di .....

2 Una rete WLAN è costituita da ..... (STA) e ..... (AP).

3 Le wireless LAN sono regolate dallo standard .....: dalla ..... in poi sono anche chiamate semplicemente ....., marchio definito da un consorzio di imprese che ormai è divenuto sinonimo di wireless.

4 L'..... (UMTS) trasmette con data rate fino a ..... su frequenze di trasmissione comprese fra ..... e ..... e rende disponibili nuovi servizi quali ..... e .....

5 Con WiMAX si intendono sistemi basati sullo standard ....., conosciuto anche come ..... .

6 L'IEEE 802.11 legacy detta le specifiche a livello ..... e di ..... per l'implementazione di una rete ..... .

2. Vero o falso

1 WAP e GPRS permettono la realizzazione di reti di dati wireless a lungo raggio. V F

2 La IEEE stabilì nel 1987 il comitato 802.11 appositamente per le WLAN. V F

3 Con Body Area Network si intendono le reti wearable, cioè indossabili. V F

4 Le Personal Area Network sono reti con area di copertura al massimo di due metri. V F

5 I dispositivi mobili nella PAN generalmente si connettono con tecnologie a infrarossi o radio. V F

6 Le specifiche per il Bluetooth rientrano nello standard IEEE 802.15. V F

7 I Wireless Terminal WT sono terminali mobili dotati di una interfaccia 802.11. V F

8 Le soluzioni WWAN si basano su un'infrastruttura a rete cellulare o su trasmissione satellitare. V F

9 La seconda generazione (3G) è caratterizzata dall'UMTS. V F

10 In Europa la banda disponibile per il 802.11 è suddivisa in 13 canali ciascuno "largo" 22 GHz. V F

11 Il protocollo 802.11f è anche chiamato IAPP (Inter Access Point Protocol). V F

12 Lo standard HomeRF viene utilizzato per trasmissioni con frequenza tipica di lavoro a 2,4 GHz e bitrate a 1,6 Mbps. V F

13 Le HiperLAN utilizzano una frequenza di 5,4 GHz con bit rate sino a 54 Mbps. V F

14 DECT fornisce servizi sia voce che dati utilizzando una frequenza che va da 2 GHz a 5 GHz. V F

LEZIONE 2

L'autenticazione nelle reti wireless

In questa lezione impareremo...

- i meccanismi WEP, WPA e WPA2
- il sistema di autenticazione 802:1X
- il protocollo EAP

La sicurezza delle reti wireless

Come ogni comunicazione cablata, la trasmissione senza fili presenta da sempre diverse problematiche relative alla sicurezza, soprattutto per il fatto che non necessita di una connessione fisica per poter accedere alla LAN.

Le reti wireless, trasmettendo dati per mezzo delle onde radio, presentano quindi ulteriori problemi rispetto alle reti wired, dipendenti proprio dalle caratteristiche del canale di comunicazione che utilizzano: una trasmissione nell'etere viene facilmente intercettata e chiunque riesce a manipolare i dati con semplici pacchetti software di pubblico dominio.

Esistono sistemi operativi basati su Ubuntu e progettati per eseguire penetration tests e un hacker, dopo aver attivato la propria scheda di rete wireless in modalità passiva (monitor mode), avvia questi sistemi operativi, magari in modalità live CD, in modo da non lasciare nessuna traccia sul computer utilizzato per il tentativo di intrusione.

> In modalità passiva la scheda di rete intercetta tutti i pacchetti emessi da un router o dalla scheda di rete di altri computer: una volta scoperto l'SSID della rete a cui connettersi, il pirata attiva uno sniffer per catturare i pacchetti necessari a portare a termine l'attacco mediante software come aircrack-ng per estrarre le password di accesso alla rete.

È necessario quindi sviluppare un insieme di meccanismi aggiuntivi per la protezione delle comunicazioni.

Sappiamo che i problemi principali che riguardano una WLAN si possono suddividere in tre categorie:
- riservatezza: i dati trasmessi attraverso il canale non devono essere intercettati e interpretati;
- controllo di accesso (Access Control): alla rete possono accedere solo gli host autorizzati;

- integrità dei dati: i messaggi trasmessi non devono essere manomessi, cioè devono giungere integri a destinazione.

Le tipologie di attacchi alle rete wireless si possono suddividere in:
- eavesdropping (intercettazione): con questo termine si indica la possibilità che entità non autorizzate riescano a intercettare e ascoltare in maniera fraudolenta i segnali radio scambiati tra una stazione wireless e un Access Point;
- accessi non autorizzati: un intruso si intromette illegalmente alla rete senza averne la autorizzazione e, una volta connesso, viola la riservatezza portando a termine degli attacchi alle risorse e alle applicazioni condivise dagli utenti della rete e immette traffico di rete non previsto;
- interferenze e jamming: tutte le apparecchiature in grado di emettere segnali a radiofrequenza entro la banda di funzionamento della rete rappresentano potenziali sorgenti di interferenza: se esiste al volontarietà di queste emissioni attaccanti e/o per disturbare la comunicazione radio si parla di jamming;
- danni materiali: posso essere fatti danni materiali allo scopo di creare malfunzionamenti o interruzioni dei servizi (Denial of Service DoS) danneggiando gli elementi che compongono la rete come gli Access Point, le antenne, i cavi dei ripetitori Wi-Fi; anche la natura può portare limitazioni o interruzioni dei servizi dato che le onde elettromagnetiche sono sensibili alle condizioni ambientali sfavorevoli come il vento, le pioggia, le neve e le temperature rigide molto fredde.

> Per la legislatura italiana è illegale procurarsi un accesso a una rete senza averne avuto l'autorizzazione e quindi questi attacchi sono configurabili come reati e di seguito sarà descritto il loro inquadramento ai sensi del Codice Penale.

La crittografia dei dati

Una soluzione alla esigenza di riservatezza è quella di criptare i dati trasmessi: l'operazione di codifica dei dati fornisce riservatezza e integrità al sistema nelle operazioni di trasmissione, mentre l'autenticazione dell'utente fornisce la disponibilità e il controllo dell'accesso alla rete.

Wired Equivalent Privacy (WEP)

Le specifiche dello standard IEEE 802.11 definiscono un meccanismo per la riservatezza dei dati conosciuto con il nome di Wired Equivalent Privacy (WEP), dato che l'obiettivo è quello di raggiungere per le reti wireless la stessa affidabilità delle reti cablate ethernet.

È un protocollo di sicurezza a livello Data Link della pila ISO-OSI che si avvale di due meccanismi aggiuntivi:
- l'algoritmo crittografico RC4;
- il sistema di controllo dell'integrità dei dati CRC-32.

La crittografia utilizzata dal protocollo WEP si basa sul modello *a chiave simmetrica* mediante un algoritmo che permette di modificare un blocco di testo in chiaro (plaintext) calcolandone lo XOR bit a bit con una chiave di cifratura pseudocasuale di uguale lunghezza (keystream).

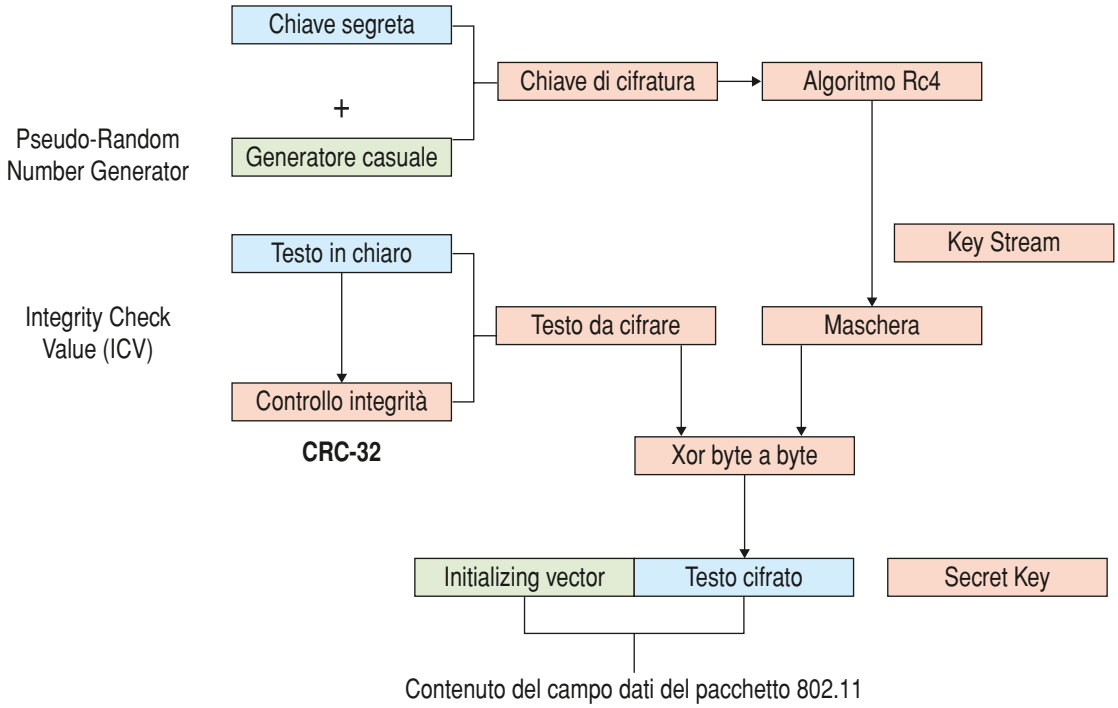
Il processo di codifica/decodifica prevede la presenza di una *chiave segreta* che costituisce uno degli input fondamentali dell'algoritmo e questa *chiave segreta* deve essere condivisa attraverso canali esterni alla rete wireless: questa necessità si traduce in un primo punto di insicurezza dell'intero

sistema, poiché bisognerà prevedere delle pratiche adeguate di conservazione e condivisione delle chiavi, nonché una rigenerazione frequente delle stesse, cosa che raramente accade nella realtà nonostante la previsione da parte del legislatore di termini brevi per la sostituzione delle password di accesso ai sistemi informatici su cui risiedono dati personali.

Analizziamo ora nel dettaglio il protocollo nella sua fase di codifica come descritto nello schema sotto riportato.

Codifica

La modalità con cui la chiave segreta viene scelta e distribuita agli host della rete non è specificata dal protocollo e dunque la sua gestione è di competenza dell'amministratore di rete che deve provvedere a comunicarla a tutti gli host che devono connettersi.



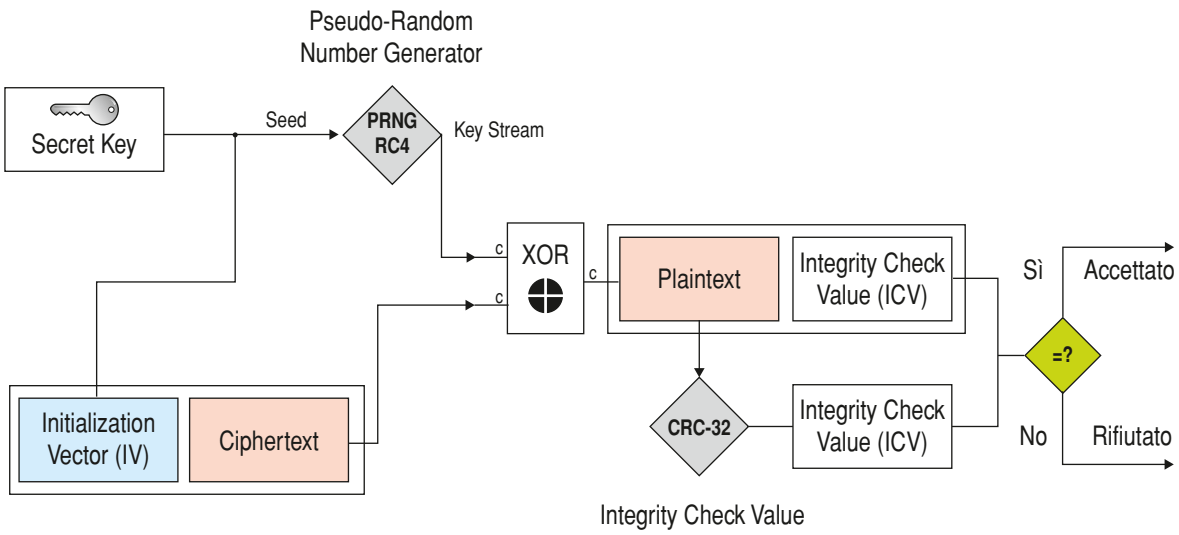
La *chiave di cifratura* viene realizzata a partire dalla *chiave segreta* che viene concatenata con un initialization vector (IV), che è un numero casuale di 24 bit, producendo l'input (seed) per il generatore pseudo casuale PRNG (pseudo-random number generator), che è la funzione più importante svolta dell'algoritmo crittografico RC4 (Rivest Chipher 4); l'RC4 produce in output la stringa denominata keystream k di lunghezza esattamente uguale a quella del messaggio che deve essere trasmesso in rete, dato che deve essere eseguito lo XOR bit a bit con esso.

Prima di essere spedito il plaintext viene analizzato e, tramite l'algoritmo CRC-32, viene generata una stringa per il controllo di parità, denominata Integrity Check Value (ICV), che viene utilizzata in ricezione per il controllo di integrità: testo e ICV vengono concatenati e sottoposti allo XOR con il keystream k, originando il testo cifrato denominato ciphertext.

Al messaggio finale viene aggiunto in chiaro l'IV iniziale, necessario per la decodifica da parte del destinatario.

Decodifica

Per effettuare la decodifica è necessario ricostruire lo stesso keystream k utilizzato in codifica: a tal fine si prende l'IV in chiaro del messaggio ricevuto, lo si concatena alla chiave segreta in possesso del destinatario e si ottiene un seed da utilizzare come input dell'algoritmo PRGN: questo, avendo le stesso input che ha utilizzato il mittente per la codifica, genererà come output lo stesso keystream k.



Ora si procede eseguendo l'operazione di XOR con il ciphertext: sfruttando l'invertibilità dell'operazione si ottiene il plaintext che viene sottoposto alla verifica di integrità mediante la ricostruzione del CRC-32 e confrontandolo col l'ICV contenuto nel messaggio ricevuto.

Sicurezza del WEP

Il WEP venne rilasciato e integrato tra le specifiche di sicurezza delle reti Wi-Fi troppo velocemente senza aver terminato gli appropriati studi sulla sua robustezza e capacità di resistere ad attacchi esterni mirati a scoprire la chiave di codifica.

Soltanto dopo l'immissione sul mercato di migliaia di dispositivi equipaggiati con tale metodo di protezione si dimostrò che la sua sicurezza offerta non era assolutamente assimilabile a quella delle reti cablate, e che normali utenti informatici grazie a software "appropriati" avrebbero potuto violare in pochissimo tempo la crittografia utilizzata dai dispositivi 802.11 e impadronirsi del traffico circolante sulla rete.

La debolezza consiste nell'uso del Vettore di Inizializzazione IV: l'algoritmo RC4, infatti, risulta vulnerabile se vengono utilizzate le chiavi per più di una volta ed è quello che accade con il WEP che ammette uno spazio di sole 224 combinazioni: bastano 5 milioni di frame per riuscire a ricavare la chiave WEP.

Wireless Protected Access (WPA-WPA2): generalità

Per sopperire all'insicurezza del WEP, anche per effetto della diffusione sempre più elevata di dispositivi senza fili che richiede la necessità di un continuo sviluppo di protocolli di sicurezza, nell'aprile del 2004 venne così istituita una task force denominata "Task Group i" con il compito di ridefinire le politiche di sicurezza dello standard IEEE 802.11.

Il protocollo che nacque venne chiamato Wireless Protected Access (WPA), rappresenta solo alcune delle funzioni presenti nello standard IEEE 802.11i, e viene implementato in due diverse configurazioni:
- modalità Personal (WPA-PSK);
- modalità Enterprise (WPA-EAP);

dove la modalità Personal viene pensata per le applicazioni SOHO (Small Office Home Office) e piccole reti, mentre la modalità Enterprise per soluzioni aziendali e infrastrutture di rete di grandi dimensioni.

Le principali migliorie introdotte dal WPA rispetto a WEP sono nelle dimensioni della chiave (128 bit) e del vettore di inizializzazione IV (48 bit) per cifrare i dati oltre all'aggiunta di un sistema di autenticazione reciproco tra client e rete wireless.

WPA utilizza inoltre un nuovo protocollo, il Temporary Key Integrity Protocol (TKIP), che permette di cambiare le chiavi crittografiche utilizzate dopo un certo numero di dati scambiati.
Al posto del CRC-32 viene utilizzato il Message Integrity Code (MIC) per effettuare il controllo dell'integrità dei dati, che in WPA prende il nome di "Michael".
Altra novità del protocollo è la netta suddivisione tra la fase che effettua la crittografia dei dati e la fase di autenticazione dei client di rete.

> Il protocollo che sfrutta completamente le funzionalità dell'IEEE 802.11i nacque nel giugno 2004, venne chiamato Wireless Protected Access 2 (WPA2) e utilizza un diverso meccanismo di cifratura:
> - WPA utilizza l'algoritmo RC4;
> - WPA2 utilizza l'algoritmo AES.

L'RC4 fu utilizzato nel WPA in quanto la Wi-Fi Alliance decise in un primo tempo di riutilizzare l'hardware dei dispositivi già diffusi sul mercato che implementavano WEP.

WPA (TKIP)

WPA utilizza un sistema software di criptaggio e di sicurezza dei dati chiamato Temporary Key Integrity Protocol (TKIP) che a tutti gli effetti si comporta da "involucro" attorno al preesistente meccanismo WEP rendendolo così un sottocomponente del processo.

È composto dai seguenti elementi:
1. meccanismo di controllo dell'integrità dei dati crittografati Michael (MIC);
2. sistema di sequenziamento dei pacchetti trasmessi;
3. sistema di rimescolamento delle chiavi;
4. meccanismo di ri-generazione casuale delle chiavi durante il processo (distribuzione dinamica).

TKIP

Il sistema TKIP non utilizza mai lo stesso valore di IV più di una volta per ogni chiave di sessione fino a che non le esaurisce tutte generandole in modo casuale: il destinatario del flusso scarta tutti i pacchetti il cui valore è già stato utilizzato come IV e criptato con la stessa chiave.

Sia il mittente che il destinatario inizializzano lo spazio di sequenziamento a zero quando si scambiano una nuova chiave k, e il mittente incrementa il numero sequenziale a ogni pacchetto inviato (sequenziamento dei pacchetti).

TKIP trasforma inoltre una chiave temporanea e un contatore sequenziale di pacchetti in una chiave di cifratura utilizzabile per una sola sequenza: quindi l'architettura TGi (Task Group i) per la generazione di chiavi dipende da una gerarchia di almeno tre tipi di chiave: chiavi temporanee, chiavi di cifratura e chiavi "master" (chiave condivisa tra i clients della rete e il server di autenticazione 802:1X).

MIC

Il MIC è un dispositivo crittografico per rilevare la presenza di messaggi falsi nella comunicazione, cioè un Message Authentication Codes (MAC): include CBC-MAC, costituito da un cipher block e ampiamente usato nelle applicazioni bancarie, e HMAC utilizzato da Internet Protocol Security (Ipsec).

Il sistema è composto da tre componenti: una chiave segreta k formata da 64 bit nota solo a mittente e destinatario, una funzione di etichettatura e un attributo di verifica.

La funzione di etichettatura E prende in input la chiave k e il messaggio M da inviare sulla rete, genera come output un'etichetta T, chiamata anche "codice di integrità" del messaggio, che viene inviata assieme al messaggio: il destinatario ripete lo stesso procedimento per verificarne l'autenticità e, in caso positivo, restituisce come risultato il valore logico TRUE, altrimenti FALSE presumendo che il messaggio ricevuto sia stato manipolato.

WPA2 (AES)

La differenza con il WPA è l'adozione di un nuovo algoritmo di sicurezza, il più diffuso al mondo tra gli algoritmi a chiave simmetrica: l'Advanced Encryption Standard (AES).

Essendo a chiave simmetrica, l'algoritmo utilizza la stessa chiave sia per la codifica che per la decodifica dei dati, con lunghezze di chiavi pari a 128, 192 e 256 bits.

AES può avere diverse modalità di utilizzo, chiamate modalità operative: una modalità operativa è una precisa "ricetta» per utilizzare l'algoritmo e sbagliare qualche passo di tale "ricetta" può compromettere la garanzia di sicurezza della cifratura.

Le modalità operative più note sono:
- Electronic Codebook (ECB);
- Counter (CTR);
- Cipher-Block Chaining (CBC).

Senza entrare nel dettaglio delle singole modalità, quella che viene maggiormente utilizzata è la CBC alla quale spesso viene aggiunto un controllo di integrità dei dati MIC per offrire maggiori garanzie sulla trasmissione dei messaggi (la modalità assume il nome di CBC-MAC).

> Il sistema AES è stato descritto in questo volume nella lezione 4 dell'unità di apprendimento 2 dedicata alla crittografia.

Autenticazione

Nell'ambito informatico il termine ◀ autenticazione ▶ assume un preciso significato, e cioè quello così definito:

◀ L'autenticazione è il processo tramite il quale un computer, un software o un utente, verifica la corretta, o almeno presunta, identità di un altro computer, software o utente che vuole comunicare attraverso una connessione. ▶

Un esempio che tutti noi effettuiamo tutti i giorni è la comune procedura di "login» per accedere a un sistema di elaborazione oppure a una sezione riservata di un portale Web, dove solo gli utenti autorizzati possono accedere.
Durante una comunicazione in rete è fondamentale che entrambi gli interlocutori siano riconosciuti: l'identità del richiedente di un servizio deve essere nota per premettergli l'accesso ai dati e alle risorse e, d'altra parte, anche il destinatario deve essere noto, in quanto bisogna essere sicuri della identità del soggetto al quale il mittente sta inviando i propri dati.

Il termine autorizzazione viene spesso identificato con autenticazione: i protocolli per la sicurezza standard, ad esempio, si basano su questo presupposto, ma in alcuni casi queste due azioni vengono affrontate con strategie differenti.

Il Sistema di autenticazione 802:1X

La prima forma di autenticazione si basava sulla conoscenza del SSID della rete: prende il nome di OSA, cioè (Open Systems Authentication), dove l'Access Point autorizzava chiunque fosse a conoscenza del SSID della rete che, però, "essendo trasmesso in chiaro", veniva subito individuato dagli sniffer.

La protezione WEP statica, ancora oggi molto utilizzata da privati e aziende per l'accesso alle reti wireless, si basa sulla condivisione della password segreta (o chiave condivisa) per l'autenticazione dell'utente nella WLAN: basta quindi conoscere chiave segreta per accedere alla rete.

Ma lo standard WEP non prevede un metodo per l'automazione dell'aggiornamento o della distribuzione di tali chiavi, quindi risulta estremamente difficile modificarle periodicamente: generalmente la chiave di accesso rimane la stessa per mesi (o anni)!

Un sistema di autenticazione aggiuntivo è quello che si basa sul filtraggio dei MAC Address dei dispositivi wireless, ma prevede una lunga procedura manuale a opera degli amministratori di rete: ma la crittografia WEP non codifica il campo dell'indirizzo MAC del frame e quindi un hacker è in grado di monitorare il traffico di una rete e individuare indirizzi MAC validi e abilitati.

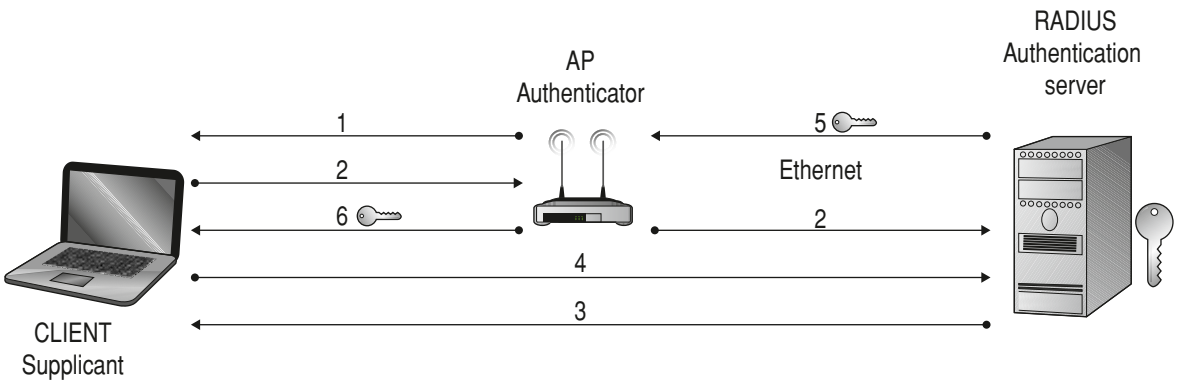
Per garantire un metodo più affidabile di autenticazione e autorizzazione, l'IEEE 802.11i ha proposto una struttura di protezione WLAN basata sul protocollo 802.1X, uno standard per l'autenticazione dell'accesso alla rete che si basa sulla gestione delle porte (Port based Network Access Control) e che viene utilizzato per la gestione delle chiavi di protezione del traffico di rete.

Oltre alle reti senza fili, il protocollo 802.1X viene implementato in numerosi switch di fascia alta della rete LAN cablata.

I componenti del sistema di autenticazione previsto dal protocollo 802.1X sono:
- l'utente di rete (supplicant);
- un dispositivo di accesso alla rete (o gateway) come un punto di accesso senza fili (authenticator);
- un servizio di autenticazione, autorizzazione e accesso (AAA) costituito generalmente da un server RADIUS (Remote Authentication Dial In User Service).

Tra supplicant e authenticator viene definito un collegamento come fosse "una connessione", chiamata "porta", nella quale viene impedito l'inoltro del traffico dei dati senza una chiave di autenticazione valida che viene gestita dal server RADIUS, che detiene le credenziali dell'utente e di autorizzazione dell'accesso alla WLAN.

Il seguente schema ci aiuta a seguire il processo necessario per ottenere una chiave di autenticazione valida:



1. un client senza fili entra nel raggio di azione di un AP senza fili: questo richiede le credenziali di accesso al client;
2. il client wireless si identifica all'AP, che inoltra le informazioni ricevute a un server RADIUS;
3. il server RADIUS richiede altre credenziali del client per verificarne l'identità, specificando il tipo di credenziali necessarie;
4. il client invia le proprie credenziali al server RADIUS;
5. il server RADIUS verifica le credenziali del client: se le credenziali sono valide, il server RADIUS invia una chiave di autenticazione crittografata al punto di accesso;
6. l'AP utilizza la chiave di autenticazione per trasmettere in modo protetto le chiavi di autenticazione.

Lo standard WPA prevede quindi due modalità di autenticazione:
- la prima basata su 802:1X e sull'autenticazione RADIUS appena descritta;
- la seconda, la WPA-PSK, che propone uno schema più semplice per ambienti SOHO utilizzando una passphrase (PSK) precondivisa senza incappare nelle note vulnerabilità dell'WEP statico.

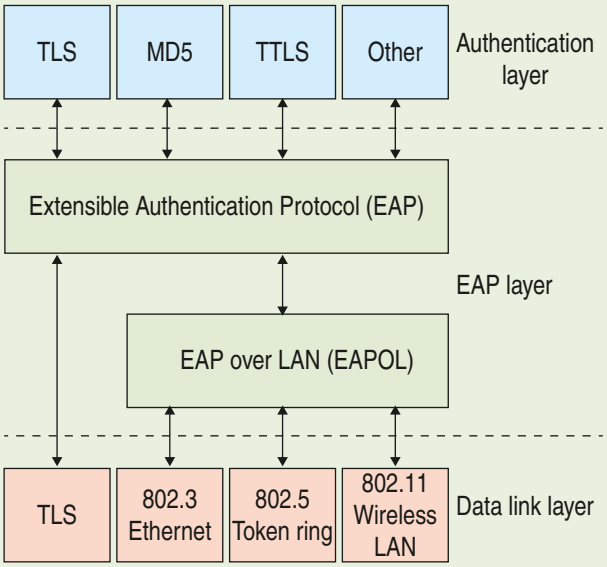
Zoom su...

EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)

Per gestire lo scambio di dati di autenticazione tra il client e il server RADIUS inoltrati dal punto di accesso, lo standard 1X si basa su un protocollo denominato EAP (Extensible Authentication Protocol): originariamente questo protocollo fu proposto come fase di autenticazione opzionale per il protocollo PPP (Point-to-point Protocol) dopo l'instaurarsi di una connessione.
Ogni meccanismo indicato in figura si basa su EAP e può quindi essere utilizzato a livello "Autenticazione" (Authentication layer) senza effettuare una pre-negoziazione: l'AP (authenticator) invia una richiesta di identificazione, request identity seguita da una o più richieste di autenticazione del client (supplicant).

Un frame di richiesta contiene un campo "tipo", per indicare quali sono le informazioni necessarie per l'autenticazione: alla sua ricezione il client invia una risposta per ogni request settando il campo "tipo" con le informazioni necessarie.

È un protocollo di autenticazione multiscopo che supporta numerosi metodi di autenticazione come token card, Kerberos, one-time password, certificate, public key authentication e smart card.



I principali tipi di AEP sono :

- EAP Message Digest 5 (EAP-MD5): si basa principalmente sull'uso di una funzione hash "one-way";
- EAP Transport Layer Security (EAP-TLS): si basa sul protocollo TLS come dice il nome stesso;
- EAP Tunneled Transport Layer Security (EAP-TTLS): la modalità di autenticazione EAP-TTLS estende EAP-TLS permettendo lo scambio di informazioni aggiuntive tra client e server, utilizzando il tunnel di comunicazione stabilito con l'uso del protocollo TLS.
- Protected Extensible Authentication Protocol (PEAP): fornisce un tunnel di comunicazione criptato e autenticato come TLS, quindi i messaggi EAP incapsulati all'interno del tunnel TLS sono protetti contro svariati attacchi;
- Microsoftc Challenge Handshake Authentication Protocol vers.2 (MS-CHAPv.2): è il protocollo di autenticazione sviluppato dall'azienda Microsoft basato sull'architettura del meccanismo CHAP (Challenge Handshake Authentication Protocol), che è uno schema di autenticazione usato dai server PPP per convalidare l'identità dei client remoti.

Il numero di *request-response* che vengono scambiati dal protocollo varia a seconda del meccanismo di autenticazione scelto: il server di autenticazione invia al client una autorizzazione positiva o negativa di accesso alla rete dopo aver analizzato tutte le informazioni richieste.

Verifichiamo le conoscenze

1. Completamento

1 Sappiamo che i problemi principali che riguardano una WLAN si possono suddividere in tre categorie:

- .....
- .....
- .....

2 Le tipologie di attacchi alle reti wireless si possono suddividere in:

- .....
- .....
- .....

3 Le onde elettromagnetiche sono sensibili alle condizioni ambientali sfavorevoli come il ....., la ....., la ..... e le .....

4 Il protocollo Wired Equivalent Privacy si avvale di due meccanismi aggiuntivi:

- l'algoritmo crittografico .....;
- il sistema di controllo dell'integrità dei dati .....

5 Il protocollo ..... (WPA) rappresenta solo alcune delle funzioni presenti nello standard IEEE 802.11i, e viene implementato in due diverse configurazioni:

- modalità Personal (.....);
- modalità Enterprise (.....).

6 Il protocollo che sfrutta completamente le funzionalità dell'IEEE 802.11i nasce nel giugno ....., viene chiamato ..... (WPA2) e utilizza come meccanismo di cifratura dei dati l'.....

7 WPA utilizza un sistema software di criptaggio e di sicurezza dei dati chiamato ..... (TKIP) che a tutti gli effetti si comporta da "....." attorno al preesistente meccanismo ..... rendendolo così un sottocomponente del processo.

8 L'architettura TGi (Task Group i) dipende da una gerarchia di almeno tre tipi di chiave: ....

2. Vero o falso

1 Esistono sistemi operativi basati su Ubuntu e progettati per eseguire penetration tests. V F

2 Il protocollo di sicurezza Wired Equivalent Privacy (WEP) è a livello Data Link. V F

3 Il protocollo WEP indica le modalità di distribuzione della chiave segreta. V F

4 Con la chiave di cifratura viene generata una stringa per il controllo di parità, l'ICV. V F

5 La debolezza del WEB è dovuta all'uso di Vettori di Inizializzazione. V F

6 La modalità WPA-EAP viene pensata per le applicazioni SOHO. V F

7 Il Message Integrity Code (MIC) in WPA viene utilizzato al posto del CRC-32. V F

8 Il sistema TKIP utilizza lo stesso valore di IV per più di una volta per ogni chiave di sessione. V F

9 La modalità operativa WPA2 maggiormente utilizzata è la CBC. V F

10 L'OSA trasmette in SSID cifrato in modo da non essere individuato. V F

11 Il protocollo 802.1X si basa sulla gestione delle porte (Port based Network Access Control. V F

12 Un server RADIUS svolge un servizio di AAA. V F

LEZIONE 3

La trasmissione wireless

In questa lezione impareremo...

- il livello fisico e la trasmissione dei segnali wireless
- il formato del frame 802.11

Cenni sulle tecnologie trasmissive

Lo strato fisico

Le reti WLAN possono essere realizzate mediante due diverse tecnologie:

- tecnologie radio: sono quelle normalmente utilizzate e sono soggette a norme molto precise per evitare interferenze con altri servizi e problemi di inquinamento elettromagnetico con tutti i dispositivi; le bande radio di trasmissione sono spesso sature;
- tecnologie ottiche: presentano numerosi problemi su distanze superiori a qualche Km e risentono di condizioni atmosferiche particolari, come la presenza di nebbia.

Le reti WLAN radio presenti oggi sul mercato utilizzano prevalentemente la banda di frequenze ISM (Industrial Scientific Medical band) composta dalle seguenti zone:

- 902 – 928 MHz;
- 2,400 – 2,480 GHz;
- 5,150 – 5,250 GHz:

Nella seguente tabella sono riportate le caratteristiche fisiche delle varie tipologie di 802.11:

Protocollo	Modulazione	Velocità	Banda utilizzata
802.11	Infrarosso diffuso	1 o 2 Mbps	–
	FHSS	1 o 2 Mbps	2,4 GHz ISM
	DSSS	1 o 2 Mpbs	2,4 GHz ISM
802.11a	OFDM	54 Mbps (max)	5,2 GHz UNII
802.11b	HR-DSSS	11 Mbps (max)	2,4 GHz ISM
802.11g	OFDM	54 Mbps (max)	2,4 GHz ISM

La velocità viene adattata dinamicamente sulla base del rapporto segnale/disturbo: per evitare le interferenze tra dispositivi che utilizzano la stessa banda si sfrutta la tecnica spread spectrum, che consiste nell'utilizzare una banda più larga di quanto richiesto così che per i dispositivi non interessati questo venga interpretato come disturbo.

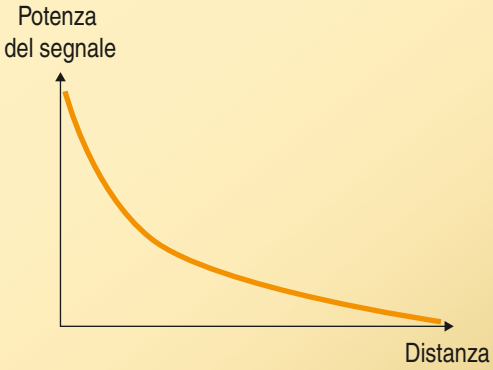
Le tecniche di modulazione utilizzate nelle trasmissione wireless sono quattro
- FHSS – Frequency Hopping Spread Spectrum;
- DSSS – Direct Sequence Spread Spectrum;
- HR DSSS – High Rate DSSS;
- OFDM – Orthogonal Frequency Division Multiplexing.

Zoom su...

MODULAZIONI

- Frequency Hopping Spread Spectrum (FHSS): nel sistema FHSS il segnale modulato di tipo FKS o GFKS a una data frequenza viene fatto "saltare" da una canale all'altro, distribuendosi su una banda di frequenze.
- Direct Sequence Spread Spectrum (DSSS): il sistema DSSS è una tecnologia di trasmissione a "frequenza diretta" su banda larga dove ogni bit viene trasmesso come una sequenza ridondante, detta chip.
- High Rate DSSS (HR DSSS): HR-DSSS lavora in modo analogo a DSSS, ma utilizza un diverso tipo di modulazione, il CCK (complementary code keying), che consente di raggiungere data rate più elevati.
- Orthogonal Frequency Division Multiplexing (OFDM): OFDM divide il messaggio da trasmettere in diversi sotto segnali a bassa velocità che vengono trasmessi in parallelo a diverse frequenze: da questo fatto deriva il nome *ortogonalità*.

La diffusione delle reti wireless domestiche e soprattutto in ambiente scolastico ha suscitato discussioni in merito alla pericolosità per la salute degli utenti: sicuramente le radiazioni "non fanno bene", ma un telefono cellulare irradia dalle 20 alle 2000 volte la potenza irradiata dai comuni apparati per telecomunicazioni senza fili. Più precisamente:
- potenza massima irradiata da un telefono cellulare GSM: ≈ 2 W;
- potenza massima irradiata da un apparato per telecomunicazioni senza fili in tecnologia Spread Spectrum: 0,001 ÷ 0,1 W.



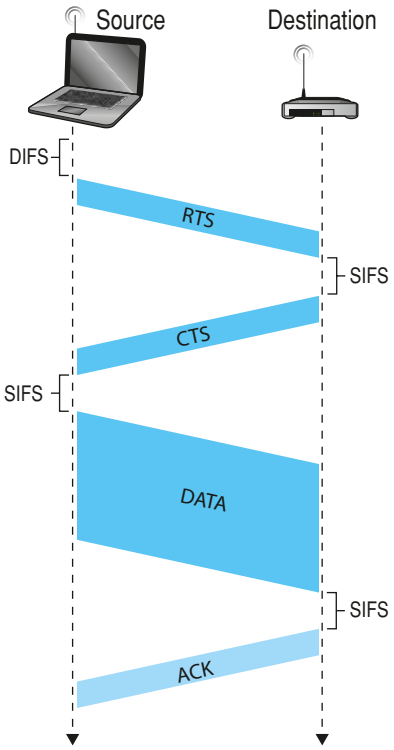
Inoltre l'intensità della radiazione emessa è inversamente proporzionale al quadrato della distanza e quindi è praticamente impossibile che un utente venga raggiunto dalla potenza massima del trasmettitore.

CDMA e CTS/RTS

Il protocollo di accesso al canale condiviso più diffuso nelle reti wireless e nelle tecnologie cellulari è lo stesso utilizzato da Ethernet, cioè Code Division Multiple Access (CDMA): un "codice" unico viene assegnato a ciascun utente (code set partitioning) che condivide con gli altri la stessa frequenza, ma ciascun utente ha una propria sequenza "chipping" per codificare i dati.

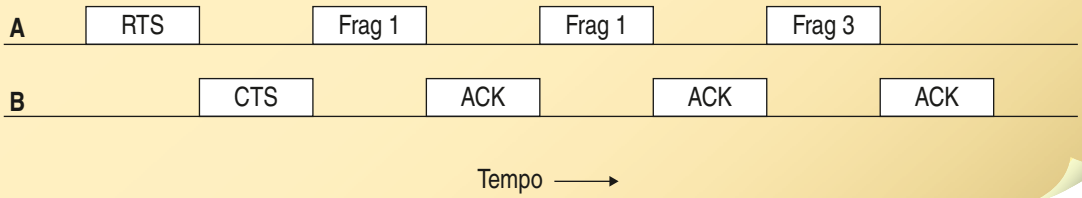
Nello standard 802.11 sono previste due modalità di funzionamento:
- DCF (Distributed Coordination Function), prevede che siano le stazioni a gestire l'accesso al mezzo trasmissivo secondo il protocollo CSMA/CA;
- PCF (Point Coordination Function) affida all'AP la coordinazione di tutte le stazioni nella sua cella (è raramente implementato).

Diversamente da Ethernet non si rilevano le collisioni anche perché c'è difficoltà in ricezione (sense collision) a causa della debolezza del segnale ricevuto (fading); per evitare collisioni durante la trasmissione è possibile per il mittente "prenotare" il canale mediante il meccanismo RTS/CTS: il mittente inizia a trasmettere un piccolo pacchetto RTS (request-to-send) all'AP usando CSMA e l'AP risponde diffondendo in broadcast il pacchetto CTS (clear-to-send) in risposta al pacchetto RTS ricevuto.
Quindi inizia a trasmettere il pacchetto di dati e, dato che CTS è ricevuto da tutti i nodi, le altre stazioni rimanderanno eventuali trasmissioni. ▶

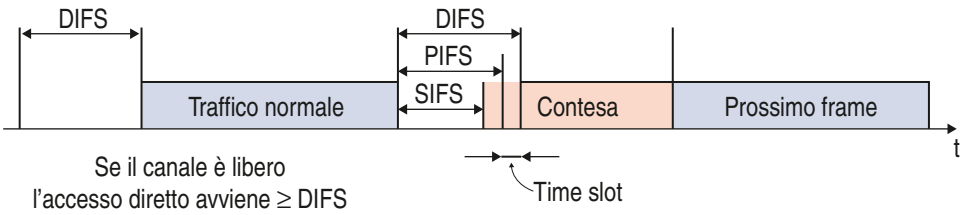


Nella modalità DCF è prevista una tecnica di frammentazione dei frame che vengono scomposti in più frammenti, ognuno numerato e riscontrato separatamente (ACK): la motivazione principale alla base di questa scelta è che essendo l'etere molto rumoroso è molto alta la probabilità che le trasmissioni vengano danneggiate e, quindi, devono essere ritrasmessi i dati: è sicuramente meglio ritrasmettere piccole porzioni piuttosto che il frame intero.

Quando il mittente acquisisce il canale con RTS e CTS può inviare in sequenza più frammenti generando quello che viene chiamato un fragment burst:



Si può osservare che tra i frame viene lasciato un intervallo di tempo (IFS Inter Frame Spacing) definito nelle specifiche MAC, che può essere di dimensioni diverse a seconda del suo utilizzo:
- DIFS (DCF, Distributed Coordination Function IFS): se l'AP non ha nulla da trasmettere, trascorso l'intervallo DIFS, ogni stazione può tentare di acquisire il canale per iniziare una nuova trasmissione (bassa priorità);
- PIFS (PCF, Point Coordination Function IFS): è l'intervallo di dimensioni medie (media priorità) utilizzato per i servizi time-bounded che utilizzano PCF;
- SIFS (Short Inter Frame Spacing): è l'intervallo più breve (alta priorità), usato per separare i frame appartenenti a una singola trasmissione, tra i frame RTS, CTS, Frag e ACK di un fragment burs.



Si può osservare che la differenza di durata tra di essi equivale a un time slot.

Lo standard 802.11 definisce anche un ulteriore intervallo di tempo, l'EIFS (Extended Inter Frame Space), che viene usato al posto di DIFS dalle stazioni che hanno ricevuto un frame incomprensibile: la sua dimensione è la maggiore di tutti ed è stata studiata in modo tale da consentire a un'altra stazione di rispondere al frame ignoto, risincronizzandola.

Quando una stazione è pronta a trasmettere inizia a effettuare il controllo del mezzo trasmissivo (etere): se lo trova libero per tutta la durata di un IFS (la cui durata dipende dal tipo di servizio come prima descritto) può iniziare a inviare i dati; se il mezzo è occupato, la stazione deve attendere un DIFS e un tempo casuale di back-off per prevenire le collisioni, multiplo di un time-slot.

Problemi nelle trasmissioni wireless

Problematiche legate alla trasmissione delle onde in etere

Riportiamo sinteticamente le principali differenze esistenti tra un sistema wireless e un sistema cablato dovute proprio al mezzo trasmissivo:

1. attenuazione del segnale: le radiazioni elettromagnetiche hanno problemi nel superare gli ostacoli e l'indebolimento della potenza del segnale è in gran parte dovuto alle proprietà degli ambienti attraversati dall'onda.
   Nella seguente tabella vengono riportati alcuni livelli di attenuazione per i diversi materiali:

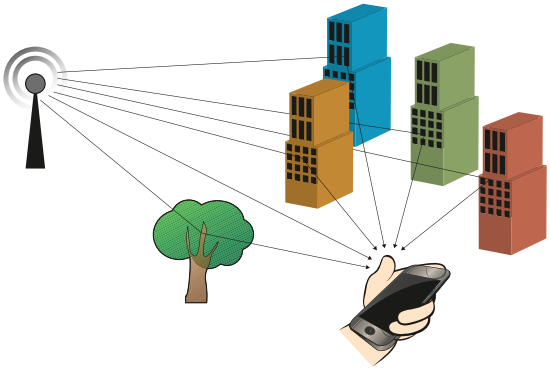
Materiali	Indebolimento	Esempi
Aria	Nessuno	Spazio aperto, cortile
Legno	Debole	Porta, tavola, separatore
Plastica	Debole	Separatore
Vetro	Debole	Finestre non colorate
Vetro colorato	Medio	Finestre colorate
Mattoni	Medio	Muri
Gesso	Medio	Separatore
Ceramica	Alto	Pavimentazione
Cemento	Alto	Muri portanti, piani, piloni
Vetro blindato	Alto	Vetri anti-proiettili
Metallo	Molto alto	Cemento armato, specchi, armadi metallici, cabine di ascensori

   nello spazio libero "libero" l'intensità del segnale si attenua al crescere della distanza (path loss);

2. interferenze da parte di altre sorgenti: l'etere è "saturo " di dispositivi che trasmettono a radiofrequenza: la frequenza wireless standard come ad esempio al 2,4 GHz è condivisa da altri dispo-

sitivi, come ad esempio la telefonia cellulare; anche rumori ambientali, come motori, trasformatori, telecomandi ecc. causano problemi legati all'interferenza dei segnali;

3 propagazione su più cammini: oltre all'assorbimento del segnale nei materiali prima descritti, il segnale si riflette su oggetti e sul terreno, compiendo cammini di diversa distanza tra trasmittente e ricevente, e quindi subisce un indebolimento dovuto alla riflessione, alla rifrazione e alla diffrazione. Quando l'onda incontra oggetti più piccoli della lunghezza d'onda, come la vegetazione, le nuvole, i segnali stradali ecc. si possono inoltre verificare problemi di ◀ scattering ▶;



◀ Scattering è il fenomeno che si verifica quando la luce colpisce le molecole sospese, ad esempio nell'aria: parte di essa viene in parte diffusa, cioè deviata dall'originaria traiettoria di propagazione, e in parte trasmessa, proseguendo il cammino lungo la stessa direzione di incidenza. ▶

4 shadowing: un problema molto frequente nei sistemi radiomobili è quello delle zone d'ombra dato che in ambito urbano, la presenza di edifici e ostacoli di ogni genere, può creare problemi nella propagazione delle onde elettromagnetiche;

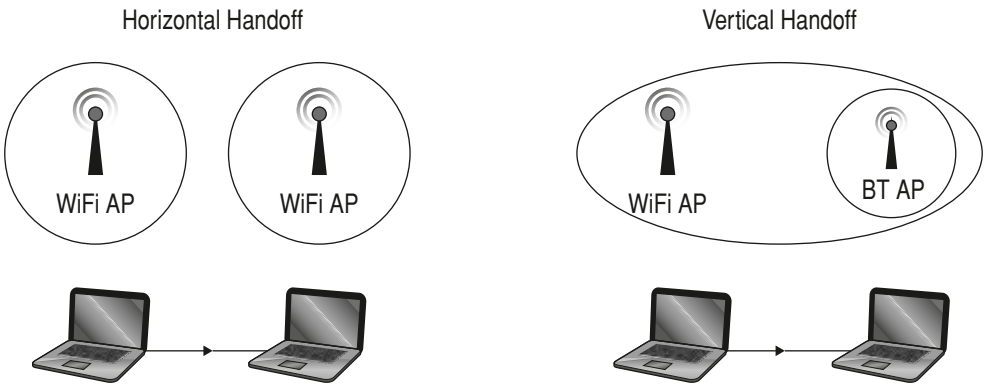
5 effetto Doppler: a causa del moto dell'utente rispetto alle stazioni radio base si verifica anche questo importante problema.

La comunicazione attraverso un collegamento wireless, persino un punto-punto, è molto più "complessa".

Problemi di posizionamento degli host

Handoff

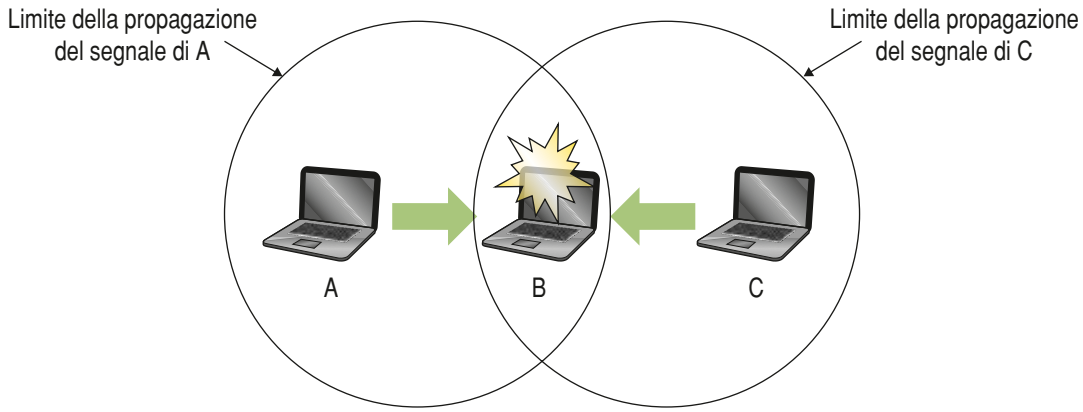
Si definisce handoff la situazione in cui l'host si sposta dall'area di copertura di una stazione base a un'altra cambiando il suo punto di collegamento con la rete globale.
Esistono due tipi di handoff: quello orizzontale, che si verifica quando un terminale effettua il passaggio tra gli AP della stessa tecnologia, e quello verticale, che si verifica quando un terminale effettua il passaggio tra gli AP di diverse tecnologie.

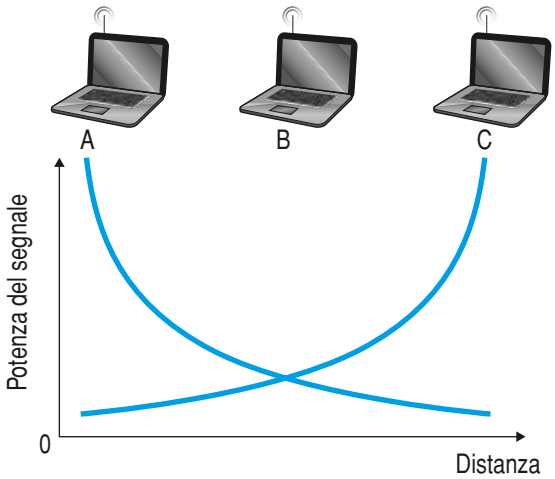


È intuitivo pensare che queste discontinuità portano a una riduzione della qualità del servizio: se ad esempio un utente sta guardando un filmato in streaming mentre si muove, a un certo punto avviene l'handoff durante il quale l'utente non riceve più i nuovi dati e quindi la visualizzazione del filmato sarà ferma all'ultimo dato ricevuto, fino al passaggio dell'handoff.

Problema della stazione nascosta (hidden terminal)

Siano date tre stazioni A, B, C con i raggi d'azione raffigurati, e A stia trasmettendo a B: se C ascolta il mezzo trasmissivo lo troverà libero e sarà convinta di poter trasmettere a B, ma cominciando a trasmettere disturberà la trasmissione di A, impedendo a B di riceverla.
Quindi sia A che C saranno costrette a ritrasmettere il messaggio: questo è noto come il problema della stazione nascosta.



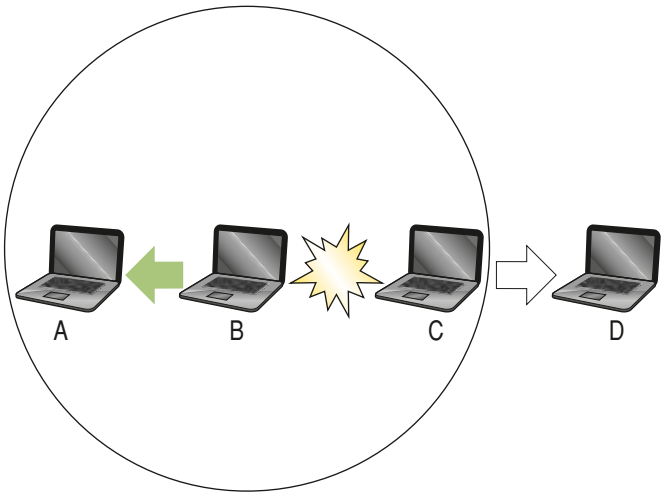


- B e A possono comunicare
- B e C possono comunicare
- A e C non possono sentirsi ma possono causare interferenza

Stazioni mittenti in collisione non sono in grado di rilevare tale condizione, ma credono che la trasmissione stia avvenendo con successo.

Problema della stazione esposta (Exposed Terminal)

È il problema inverso del precedente: supponiamo che B stia trasmettendo ad A e che C voglia trasmettere a D: ascoltando l'etere, C sentirà la trasmissione di B e concluderà erroneamente di non poter trasmettere; invece, essendo D fuori della portata di B e A fuori della portata di C, le due trasmissioni potrebbero avvenire parallelamente senza interferenze.
Questo è noto come il problema della stazione esposta.



- B sta trasmettendo ad A
- C deve trasmettere a D
- C ascolta il canale e lo trova occupato, quindi aspetta (erroneamente)

> Una stazione mittente non inizia una trasmissione, anche se quest'ultima potrebbe avvenire con successo.

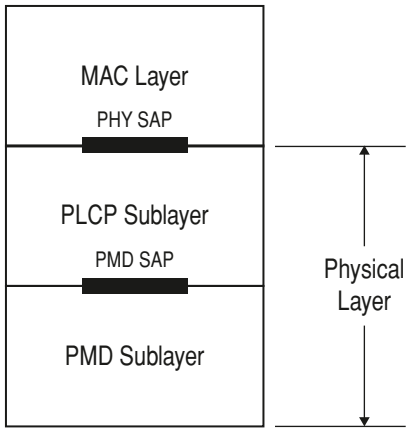
Struttura del frame 802.11

Prima di descrivere la composizione del frame 802.11 vediamo brevemente come è organizzato il livello fisico che anche nelle reti wireless ha il compito di fornire un canale per la comunicazione attraverso la definizione di specifiche relative alla parte elettrica, meccanica e procedurale.

Livello fisico (physical layer)

Nelle WLAN esistono differenti tipi di livelli fisici, ognuno dei quali si contraddistingue principalmente in base al meccanismo di trasmissione: a partire dalle prime versioni di 802.11, che si basavano su FHSS e DSSS si sono, col passare del tempo e col superamento di problemi tecnologici, implementati nuovi sistemi di trasmissione, come:

- HRDSSS: definito per 802.11b;
- OFDM: su cui si basa il più recente 802.11a.



Lo standard prevede una scomposizione in due sottolivelli per il physical layer:

- PLCP, Physical Layer Convergence Procedure: interfaccia il MAC con il livello sottostante;
- PMD, Physical Medium Dependent: provvede alla trasmissione e alla ricezione interfacciandosi al mezzo (l'etere). ▶

Al MAC giunge il frame 801.11 cosi composto:

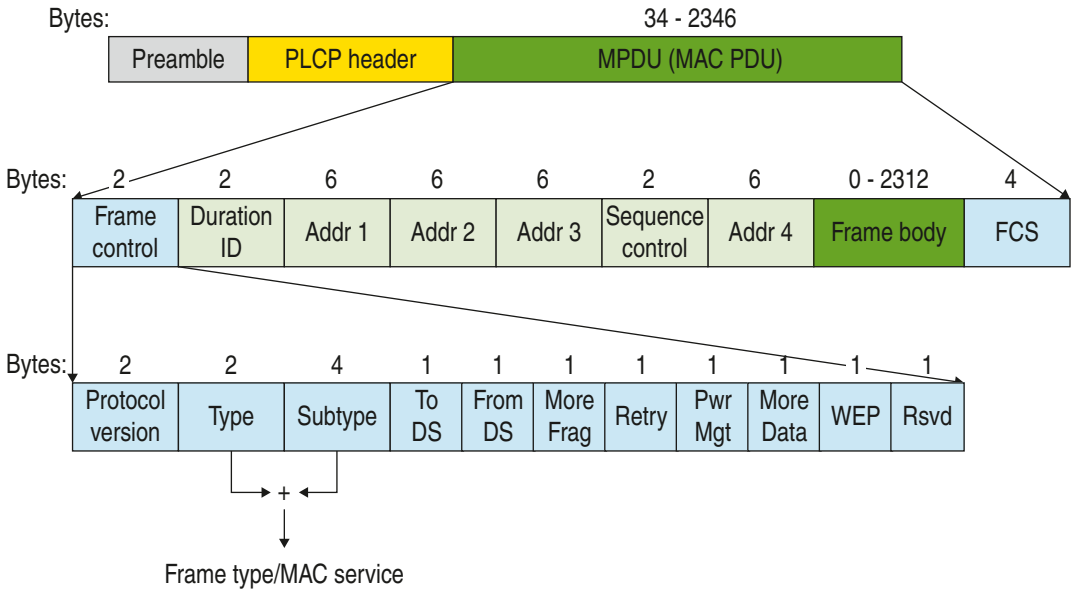
dove il PLCP Header contiene le informazioni per l'interfacciamento tra lo strato PMD e MAC ed è previsto uno specifico PLPC per le diverse tecniche di trasmissione, in particolare per:
- FHSS;
- DSSS in 802.11 (1 & 2 Mb/s);
- DSSS in 802.11a (6 ÷ 54 Mb/s);
- DSSS in 802.11b (1 ÷ 11 Mb/s);
- DSSS in 802.11g (1 ÷ 54 Mb/s);

e serve per definire la velocità operativa, il tipo di modulazione e la codifica da utilizzare per i dati.

Formato del frame

Lo standard IEEE 802.11 specifica il formato di tutti i campi dei tre tipi di frame previsti, Dati, Controllo e Gestione, aventi la stessa struttura composta da un header, un body di lunghezza variabile e un Frame Check Sequence di 32 bit (FCS).
La sequenza di bit viene passata dall'entità MAC al PLCP (Physical Layer Convergence Protocol) a partire dal primo bit del campo Frame Control fino all'ultimo bit del campo FCS.

I frame di tipo "Dati" (Data frame) hanno la struttura rappresentata in figura:



Nel dettaglio il Frame Control è composto dai seguenti campi:
- Protocol Version: zero per lo standard 802.11;
- Type: tipo di frame, che può assumere 3 valori: data, gestione, controllo;
- Subtype: sotto tipo di frame (RTS, CTS, Ack o gestione);
- ToDS: quando è settato indica che la destinazione è il Distribution System;
- FromDS: quando è settato indica che proviene dal Distribution System;
- Retry: è settato a 1 se il frame è una ritrasmissione;
- More fragments: è settato a 1 se a esso seguono altri frammenti della stessa comunicazione;
- Power Management: è settato a 1 se al termine la stazione va in Power Save mode (PS);
- More Data: è settato a 1 se l'AP ha altri dati per la stazione che è in PS;
- WEP: è settato a 1 se nel campo Frame Body ci sono dati che devono essere analizzati con l'algoritmo WEP;
- Order: se è settato a 1 indica che la trasmissione è soggetta a restrizioni.

ESEMPIO

Vediamo ad esempio il significato delle quattro possibili combinazioni dei bit ToDS e FromDS:

1 nella trasmissione tra stazioni che appartengono alla stesso BSS (Basic Server Set) si ha:

Bytes:	2	2	4	1	1	1	1	1	1	1	1
	Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Rsvd
				0	0						

2 nella trasmissione del frame da una stazione verso il Distribution System si ha:

Bytes:	2	2	4	1	1	1	1	1	1	1	1
	Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Rsvd
				1	0						

3 se il frame è proveniente dal Distribution System si ha:

Bytes:	2	2	4	1	1	1	1	1	1	1	1
	Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Rsvd
				0	1						

4 nel caso di trasmissione STA appartenente a un altro BSS, trasmessi tra AP attraverso Wireless Distribution System i due flag sono settati a 1:

Bytes:	2	2	4	1	1	1	1	1	1	1	1
	Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Rsvd
				1	1						

Il campo Duration ID consente alle stazioni che hanno ricevuto il frame di prevedere per quanto tempo il mezzo rimarrà occupato.

Gli indirizzi sono 4, in quanto, oltre agli indirizzi delle stazioni di origine e di destinazione, sono presenti anche quelli degli AP di entrata e uscita nelle comunicazioni fra celle differenti.

Bytes:	2	2	6	6	6	2	6	0 - 2312	4
	Frame control	Duration ID	Addr 1	Addr 2	Addr 3	Sequence control	Addr 4	Frame body	FCS

Gli indirizzi sono tutti nel formato standard IEEE 802 a 48 bit e hanno un diverso contenuto a seconda del valore dei bit ToDS e FromDS:

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

dove:
- DA = Destination MAC Address
- SA = Source MAC Address
- RA = Receiver Address indicate il MAC Address della stazione WM che ha ricevuto il frame
- TA = Transmitter Address indica la stazione che ha trasmesso il frame in WM
- BSSID: identificativo di 6 byte (48 bit) di ogni BSS

Il risparmio energetico nella trasmissione

I dispositivi portatili e/o mobili in generale per poter operare hanno bisogno di sorgenti esterne di energia (batterie, celle solari) che hanno notoriamente una durata che generalmente non supera le 24 ore per un utilizzo medio oltre ad avere un tempo di vita limitato.

Con l'aumentare delle prestazioni dei dispositivi portatili aumentano le richieste di energia e le aspettative di autonomia dei dispositivi da parte degli utenti: se da una parte si stanno studiando nuove tecnologie, per le batterie occorre mettere in atto tutte le tecniche possibili per cercare di evitare il più possibile sprechi di energia per massimizzare il tempo in cui i dispositivi possono essere operativi.

Se analizziamo un laptop, gli elementi che hanno un consumo energetico significativo sono il microprocessore (CPU), lo schermo LCD, l'hard disk, la system memory (DRAM), la keyboard/mouse, CDROM drive, I/O subsystem, e la wireless network interface card: l'interfaccia per le comunicazioni wireless radio è una delle componenti più significative (dopo il display) del consumo energetico.

ESEMPIO

In un laptop possiamo così ripartire il consumo energetico:
- 36% del consumo energetico è dovuto al display;
- 21% CPU+memoria;
- 18% interfaccia radio;
- 18% hard drive.

Dalla fine degli anni '90 si è iniziato a ricercare tecniche per abbassare il consumo energetico dell'interfaccia radio, sostanzialmente dovuto a due fattori:
- computazione: processing associato alle operazioni del protocollo;
- comunicazione: uso del transceiver per inviare e ricevere pacchetti dati e di controllo.

> Tra computazione e comunicazione c'è comunque un conflitto di esigenze: i protocolli a basso consumo energetico per la comunicazione tipicamente aggiungono complessità di calcolo e quindi necessitano di maggior computazione con maggior spreco di energia.

Inoltre una ulteriore problematica è legata al posto dove fisicamente viene elaborata l'informazione, cioè in locale o in rete: processare le informazioni in rete può ridurre la necessità di comunicazione ma richiede maggiore energia "consumata" dai nodi che la elaborano.

I protocolli di comunicazione a basso consumo energetico cercano di ottimizzare questi compromessi.

Verifichiamo le conoscenze

1. Completamento

1 Le reti WLAN possono essere realizzate mediante due diverse tecnologie:

- .....
- .....

2 Le tecniche di modulazione utilizzate nella trasmissione wireless sono quattro:

- .....
- .....
- .....
- .....

3 Il protocollo di accesso al canale condiviso più diffuso nelle reti wireless e nelle tecnologie cellulari è lo stesso utilizzato da Ethernet, cioè ..... che nello standard 802.11 prevede due modalità di funzionamento:

- .....
- .....

4 Il mittente prenota il canale mediante il meccanismo .....: inizia a trasmettere un piccolo pacchetto ..... all'AP usando ..... e l'AP risponde diffondendo in broadcast il pacchetto ..... in risposta al pacchetto ..... ricevuto.

5 Tra i frame viene lasciato un intervallo di tempo ..... definito nelle specifiche MAC, che può essere di dimensioni diverse a seconda del suo utilizzo:

- .....
- .....
- .....

6 Problematiche legate alla trasmissione delle onde in etere:

1 .....
2 .....
3 .....
4 .....
5 .....

7 Problematiche legate al posizionamento degli host:

1 .....
2 .....
3 .....

2. Vero o falso

1 Le reti WLAN radio utilizzano prevalentemente la banda di frequenze ISM: 2,4 ÷ 2,48 GHz. V F

2 La potenza massima irradiata da un telefono cellulare GSM: ≈ 2 W. V F

3 La potenza massima irradiata in tecnologia Spread Spectrum: 0,001 ÷ 0,1 mW. V F

4 Per evitare collisioni durante la trasmissione il mittente utilizza il meccanismo RTS/CTS. V F

5 In Ethernet si rilevano le collisioni col protocollo CSMA/CA. V F

6 Nella modalità DCF è prevista una tecnica di frammentazione dei frame. V F

7 La differenza di durata tra gli IFS equivale a un time slot. V F

8 Nel gesso l'attenuazione del segnale è maggiore che nella plastica. V F

9 Nel vetro colorato l'attenuazione del segnale è maggiore che nella plastica. V F

10 HRDSSS è definito per 802.11b mentre l'OFDM è nel più recente 802.11a. V F

LEZIONE 4

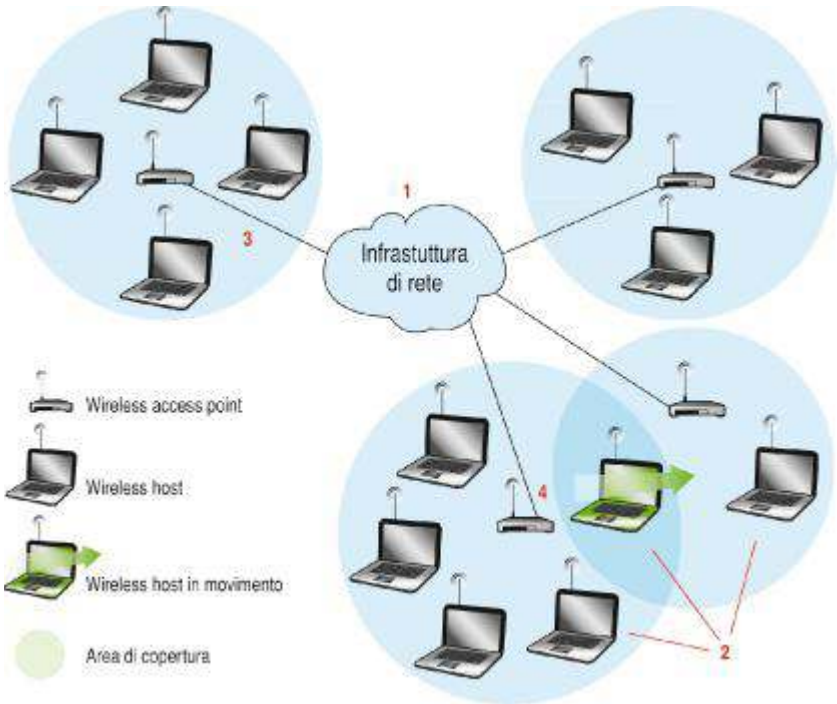
L'architettura delle reti wireless

In questa lezione impareremo...

- i componenti di una rete wireless
- le topologie e le architetture di rete wireless

Componenti di una rete wireless

Prima di definire le diverse architetture e/o topologie, individuiamo nello schema seguente i componenti di una rete wireless.



1. Infrastruttura di rete: rete con la quale l'host wireless vuole connettersi.
2. Host wireless: possono essere laptop, PDA, telefoni IP che mandano in esecuzione applicazioni TCP/IP; non necessariamente devono essere mobili (ad esempio la stampante connessa Wi-Fi).
3. Collegamenti: i dispositivi si connettono alla stazione base tramite l'etere mentre i collegamenti wired presenti nelle reti wireless sono usati per collegare la stazione base a una rete cablata: la presenza di un collegamento wired fa assumere alla rete il nome di "rete con infrastruttura".
4. Stazione base: è in genere connessa a una rete cablata e ha la funzione di ripetitore in quanto è responsabile dell'invio di pacchetti tra reti cablate e host wireless nella sua "area di copertura" (prende il nome Cell Tower nelle reti cellulari e di Access Point nelle LAN 802.11).

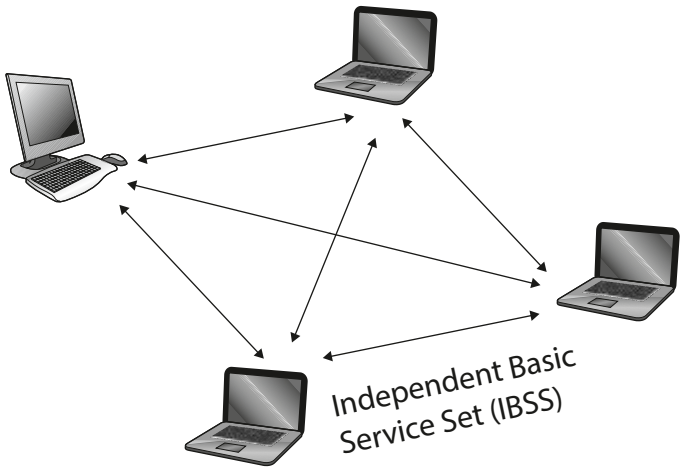
Possiamo definire la seguente tassonomia delle reti wireless:
1. hop singolo, senza infrastruttura: non è presente nessuna stazione base dato che la rete è composta da un singolo nodo che gestisce la trasmissione (esempio: Bluetooth);
2. hop singolo con infrastruttura: una stazione è collegata alla rete cablata e gli altri dispositivi sono collegati con un singolo hop tra host e stazione (esempio: rete 802.11 di casa, di una biblioteca ecc.);
3. hop multipli, senza infrastruttura: non vi è nessuna stazione base e la destinazione può essere raggiunta attraverso i nodi intermedi, che possono essere mobili (esempio: rete mobile *ad hoc*, rete veicolare *ad hoc*);
4. hop multipli con infrastruttura: un host (la stazione base) è collegata alla infrastruttura mentre i nodi si connettono wireless alla stazione base e trasmettono i dati anche tra di loro (esempio: reti di sensori wireless, reti mesh wireless).

Lo standard 802.11 definisce due topologie di rete:
- Reti IBSS (Independent Basic Service Set) o reti *ad hoc*;
- Reti ESS (Extended Service Set) o reti a "infrastruttura".

Con il termine Extended Service Set (ESS) si intende una configurazione che prevede il collegamento di due o più BSS in una singola sotto rete: più AP comunicano tra loro, consentendo una ottimizzazione del traffico tra le stazioni.

Reti IBSS o modalità *ad hoc*

La prima tipologia di reti wireless non prevede l'utilizzo di infrastrutture di supporto per la comunicazione; viene definita *ad hoc* e in essa le reti sono formate da un insieme di nodi mobili, PDA o laptop, che comunicano fra loro attraverso link wireless.



L'Independent Basic Service Set (IBSS), è la forma più semplice di rete ad hoc, composta da un insieme di STA che comunicano senza l'aiuto di una infrastruttura, e quindi ogni stazione può comunicare con un'altra stazione del medesimo IBSS senza che il traffico passi attraverso un AP centralizzato.

Nella topologia IBSS si realizzano comunicazioni peer-to-peer tra le stazioni (STA) che sono localizzate nella medesima area (BSA, Basic Service Area) e che costituiscono un insieme denominato Basic Service Set (BSS): il mezzo trasmissivo condiviso della WLAN è l'etere.

Le stazioni STA localizzate nell'area BSA sono sotto il controllo di una funzione di coordinamento che generalmente è del tipo distribuito, cioè Distributed Coordination Function DCF, e quindi la funzione DCF deve essere presente in tutte le stazioni.

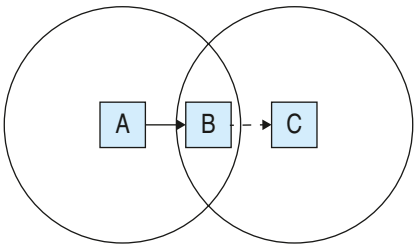
Esistono situazioni in cui viene applicato il concetto master/slave e il controllo è concentrato (PCF Point Coordination Function), dove una STA viene eletta master ed effettua il polling verso le altre stazioni.

Nel tipo distribuito i nodi della rete possono liberamente e dinamicamente organizzarsi in maniera arbitraria e temporanea permettendo agli utenti di collaborare in modo improvvisato ovunque essi si trovino: essendo formate da nodi mobili, le reti ad hoc, sono note anche con il nome di MANET (Mobile ad hoc NETwork) e sono dinamiche, nel senso che, essendo i dispositivi mobili, continuano a cambiare di numero dato che quando un host si allontana esce dal raggio di azione della rete.

Ogni nodo di una rete ad hoc opera non solo come host ma anche come router provvedendo a instradare quei pacchetti che non possono essere trasmessi direttamente al destinatario a causa del limitato raggio d'azione, che però si trovano nella sua area di raggiungibilità.

ESEMPIO

A vuole trasmettere un messaggio a C ma non è in grado di raggiungerlo: B li raggiunge entrambi e quindi può fare funzione di router instradando i pacchetti di A verso C.



Ogni host appartenente alle rete ad hoc è in grado di configurarsi in modo tale da "far rimbalzare automaticamente" le informazioni verso un altro nodo che si trova più vicino al destinatario del pacchetto: per questo motivo le MANET sono reti "multi hop" in quanto, oltre a far comunicare direttamente due nodi che si trovano a breve distanza, possono trasmettere le informazioni anche tra due nodi lontani facendo "rimbalzare" le informazioni attraverso diversi nodi intermedi.

Dato che la topologia di queste reti è in continua mutazione per le connessioni/sconnessioni dei dispositivi, i meccanismi di routing devono essere continuamente rivisti e aggiornati.

Inserimento di una stazione in un IBSS

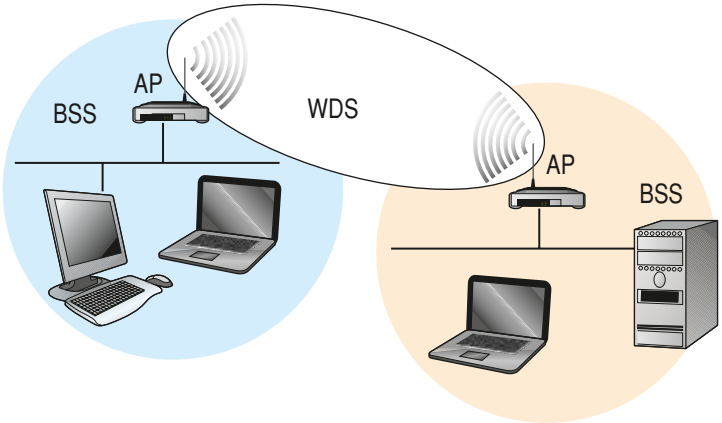
Quando una nuova stazione vuole unirsi a un BSS deve sintonizzarsi e sincronizzarsi con le altre stazioni e lo fa mediante la scansione di tutti canali, generalmente in modo passivo (passive-scanning): la stazione rimane in ascolto su ogni canale per un certo tempo in attesa che le giunga un ◀ beacon ▶ e quando le arriva ne estrae il SSID e lo confronta con quello in suo possesso per verificare se ha l'autorizzazione per connettersi a quel IBSS.

◀ I beacon sono dei pacchetti speciali di Management che contengono le informazioni di Service Set ID (SSID) e timestamp necessarie alla sincronizzazione della stazione: in una rete ad hoc tutte le stazioni partecipano alla generazione di pacchetti di beacon. ▶

Reti EES

Le reti EES, anche denominate di tipo Infrastructure, sono caratterizzate dalla presenza di una LAN di distribuzione denominata Distribution System, che interconnette diversi BSS e trasporta a livello MAC le trame: può essere cablata oppure wireless, e in questo caso prende il nome di Wireless Distribution System (WDS).

Un Access Point con l'insieme delle Stazioni a esso associati (WT Wireless Terminal) prende il nome di BSS (Basic Service Set) e costituisce una cella il cui diametro è circa il doppio della copertura/distanza tra due stazioni wireless: ciascuna cella viene identificata tramite un numero unico di 48 bit, il BSS-ID.
Nella modalità infrastruttura, il BSS-ID corrisponde all'indirizzo MAC del punto di accesso.

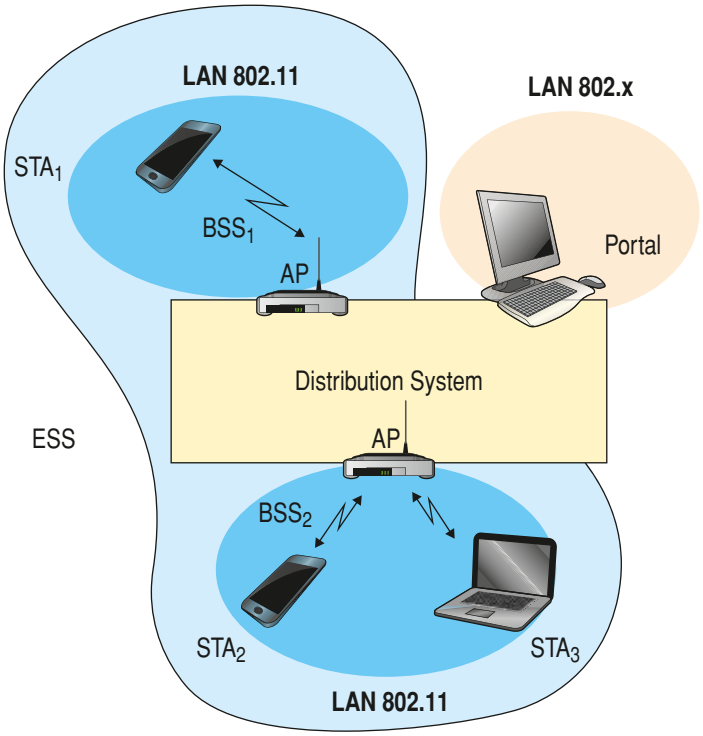


Non bisogna confondere il BSS-ID con il SSID: il primo è l'identificativo della cella mentre il secondo è il nome con cui una WLAN si identifica ai suoi utenti.

L'SSID lungo 0 corrisponde a una identità di broadcast ed è utilizzato nel probing delle reti disponibili: inoltre su alcuni AP si può inibire la trasmissione dell'SSID, in modo che solo chi conosce l'SSID della WLAN si possa associare.

L'AP coordina la trasmissione dei dati e la comunicazione tra i clients, e generalmente svolge anche la funzione di ponte tra LAN wireless, eventuali reti fisse e la rete telefonica pubblica (quindi anche Internet).
Tutto il traffico radio dei dati transita da e verso l'Access Point.

L'area coperta dal BSS è anche nota come BSA (Basic Service Area).



Le reti ESS sono costituite dall'unione di più Basic Service Set (BSS).

> L'AP può essere visto come un bridge posto tra il BSS e il DS e la BSS può essere considerata come un'unica WLAN.

Una stazione presente sul sistema di distribuzione, detta Portal, interconnette la WLAN con altre reti: è un bridge tra il Distribution System e un'altra rete wired.

I diversi BSS fisicamente possono essere locati all'interno di un ESS secondo diversi criteri:
- BSS parzialmente sovrapposti: permettono di fornire una copertura continua;
- BSS fisicamente disgiunti;
- BSS co-locati (diversi BSS nella stessa area): possono fornire una ridondanza alla rete o permettere prestazioni superiori.

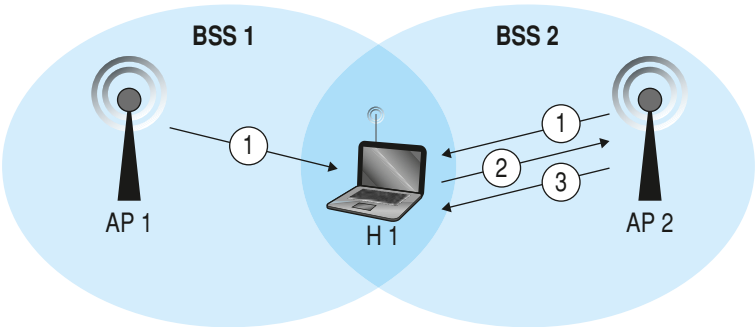
Se un dispositivo mobile è in movimento può naturalmente raggiungere il confine della sua cella e deve poter essere "agganciato" dalla cella successiva, in modo da avere la permanenza della connessione.

L'802.11 gestisce il passaggio tra stazioni con tre diverse modalità di transizioni:
- transizione tra ESS: la stazione si sposta tra BSS appartenenti a due ESS diversi: la stazione può muoversi ma non si è in grado di mantenere la connettività dato che si passa da una LAN a un'altra;
- transizione tra BSS: in questo caso la stazione si sposta tra due diversi BSS parzialmente sovrapposti appartenenti allo stesso EES: questa situazione viene gestita in maniera trasparente per i livelli superiori;
- statica: la stazione è immobile o si sposta solo entro l'area di un singolo BSS, quindi il problema non sussiste.

Scanning in una rete

I dispositivi wireless per potersi connettere "fiutano" l'etere effettuando una scansione delle possibili frequenze di trasmissione: lo scan può essere utilizzato per trovare una rete e connettersi a essa, per trovare un nuovo AP (Roaming) oppure per inizializzare una IBSS e può essere:

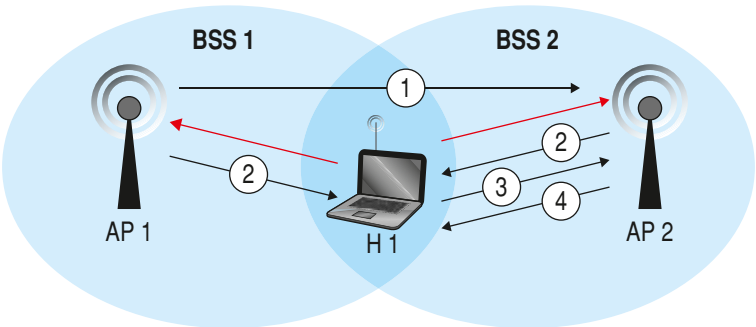
A di tipo Passive basato sulla trasmissione periodica di beacon che contengono il proprio codice SSID e il proprio indirizzo MAC (il BSS-ID);

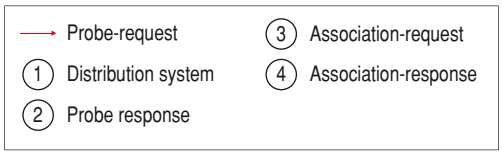


1. rimane in attesa per un certo tempo per la ricezione di un beacon;
2. la stazione seleziona l'AP migliore e invia a questo una richiesta di associazione con una trama Association-Request;
3. l'AP risponde inviando una trama Association-Response.

La STA si mette in ascolto su ciascun canale specificato nella Channel List della primitiva per il tempo specificato, aspettando di riconoscere dei frame di tipo beacon contenenti il particolare SSID scelto oppure aspettando di riconoscere un beacon con l'SSID broadcast, a seconda di quanto specificato nella primitiva stessa.

B di tipo Active, dove l'AP risponde alle richieste di sondaggio da parte delle STA attraverso i Probe-Request inviando le conferme di Probe-Response: per associarsi a un AP la stazione deve scambiare con esso tre tipi di pacchetti: un pacchetto chiamato "Probe" (dove *probe* ha il senso di sondaggio o indagine), un pacchetto di *autenticazione* e un pacchetto di *associazione*.





Questo meccanismo è adottato sulle reti di tipo di ESS in cui l'AP ha l'incarico di rispondere al probe-request. Descriviamo le operazioni che vengono eseguite da una stazione che vuole entrare a far parte di un rete:

1. invia un pacchetto di management di tipo Probe-Request in broadcast con gli identificativi della rete cercata: questo pacchetto contiene informazioni sulla stazione 802.11 come il bitrate supportato dalla stazione, il SSID di appartenenza della stazione ecc.;
2. rimane in attesa per un certo tempo di ricevere il pacchetto di Probe-Response: se non riceve risposta passa al canale successivo (nel caso in cui non abbia un canale fisso preimpostato);
3. la stazione seleziona l'AP migliore e invia a questo una richiesta di associazione con una trama Association-Request;
4. l'AP risponde inviando una trama Association-Response.

Il ruolo dell'Access Point

Possiamo dare ora la seguente definizione di ◀ Access Point ▶.

◀ Un Access Point è un'entità che permette la distribuzione dei servizi MAC via Wireless Medium (WM) per le stazioni a esso associate. ▶

In genere è una sorta di bridge locale che interfaccia la rete wireless con una wired e copre una ben determinata area consentendo ai dispositivi di passare da una cella all'altra garantendo la connettività. Può anche essere utilizzato semplicemente come ripetitore di segnale ed effettua le funzioni di bridging, fondamentali per la traduzione dei frame tra la rete wired e wireless.

L'Access Point è tipicamente un apparato con ridotte funzioni che può essere configurato per funzionare in due modalità, come "*Root Access Point*" oppure come "*Repeater Access Point*".

Root Access Point

Se viene configurato come "*Root Access Point*" realizza le funzione di DCF e di apparato di associazione per le stazioni presenti nel BSS (Active Scanning): questa è la configurazione di default che troviamo in ogni AP.

Quando una stazione viene associata all'AP, questo ne scrive l'indirizzo MAC in una tabella che mantiene aggiornata con le nuove connessioni/disconnessioni.

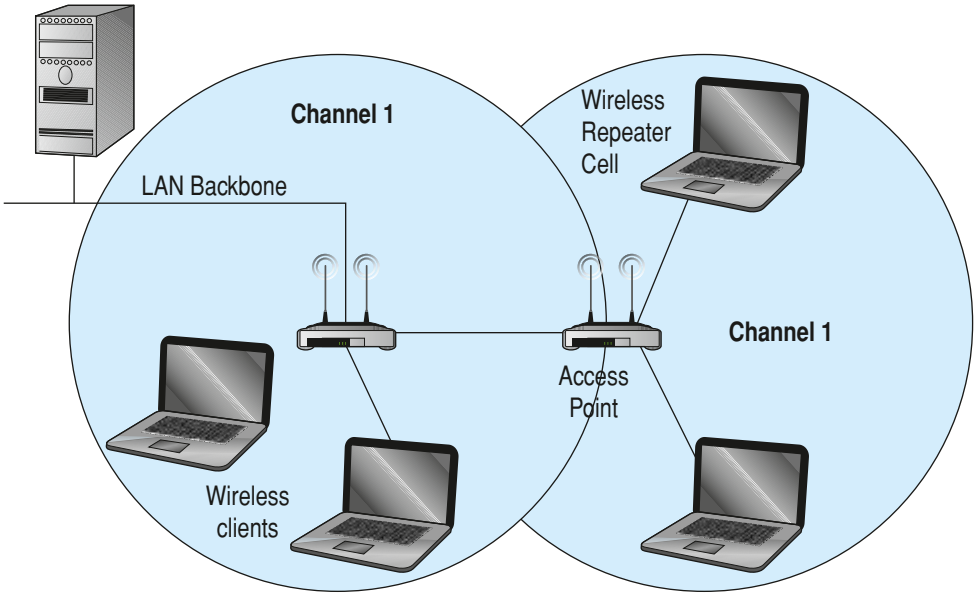
Alla ricezione di un pacchetto dal WM, se l'indirizzo MAC di destinazione è presente nella tabella delle stazioni associate al AP, il pacchetto viene ritrasmesso nel WM, altrimenti se l'indirizzo MAC di destinazione non è presente nella tabella delle stazioni associate al AP il pacchetto viene tradotto e trasmesso nella porta wired (tipicamente Ethernet).

Alla ricezione di un pacchetto dalla porta wired ha un comportamento simile a quello della Default Route: se l'indirizzo MAC di destinazione è presente nella tabella delle stazioni associate al AP il pacchetto viene tradotto e trasmesso nel WM mentre se l'indirizzo MAC di destinazione non è presente nella tabella delle stazioni associate al AP il pacchetto viene scartato.

Repeater Access Point

Se invece viene configurato come "*Repeater Access Point*", le stazioni in portata radio del Repeater risultano associate al Root Access Point e alla ricezione di un pacchetto dal WM il repeater lo ritrasmette nel WM.

L'Access Point è quindi impiegato come Repeater nel WM che permette di utilizzare lo stesso canale ripetendo le trame con peggioramento delle prestazioni della rete: la stazione che si trova nell'area di sovrapposizione si aggancia al segnale migliore.



Servizi del Distribution System

Anche se nello standard 802.11 il DS non è esplicitamente specificato, sono specificati i servizi che il DS deve supportare e sono divisi in due sezioni:

- Distribution System Services (DSS);
- Station Services (SS).

La SS vale per entrambe le modalità di costituzione della WLAN mentre la DSS vale solo per le WLAN a infrastruttura: i "servizi di distribuzione" sono forniti dall'AP mentre i "servizi host" devono essere assolti da tutte le stazioni.

DSS (servizi di distribuzione)

1. association (associazione): appena una stazione entra nel raggio d'azione di un AP, invoca questo servizio per informare la stazione base della sua presenza nella BSS e comunica le proprie necessità; una STA non può associarsi con più di un AP in uno stesso momento, questo per assicurare che il servizio di distribuzione trovi un AP unico per trasportare i messaggi del DS;
2. disassociation (dissociazione): sia le stazioni che gli AP possono terminare una precedente associazione; è una *notifica*, non una richiesta e quindi non può essere *rifiutata* da nessuna delle due parti;
3. reassociation (riassociazione): in una stazione in moto per supportare la transizione di tipo "BSS-transition" è necessario invocare il servizio di riassociazione in modo da trasferire il controllo da un AP all'altro; questo tiene informato il DS della mappa tra AP e STA quando quest'ultima si sposta da una BSS a un'altra;
4. distribution (distribuzione): viene utilizzato dalle stazioni per scambiarsi pacchetti che devono attraversare il DS: l'AP conosce la posizione delle diverse stazioni grazie al servizio di Association ed è in grado di smistare i frame che lo raggiungono verso le stazioni della propria cella (via radio) o verso gli altri AP, attraverso il sistema di distribuzione;
5. integration (integrazione): questo servizio gestisce la traduzione dei frame 802.11 verso le altre LAN IEEE 802.x. che utilizzano altri formati; il servizio di Integration provvede all'eventuale traduzione degli indirizzi e all'adattamento ai diversi media.

SS (Servizi host)

6. Authentication (autenticazione): una stazione deve dimostrare di essere autorizzata a usufruire del servizio di trasmissione e l'AP deve a sua volta farsi riconoscere: un esempio di schema di autenticazione supportato è lo schema "a chiave condivisa" (shared key);
7. deauthentication (de autenticazione): una stazione che voglia abbandonare la rete deve "de-autenticarsi" e "dissociarsi"; la de-autenticazione è una *notifica*, non una richiesta e quindi non può essere *rifiutata* da nessuna delle due parti;
8. privacy (segretezza): bisogna raggiungere un livello di riservatezza dei dati paragonabile a quello di una rete cablata dato che i dati trasmessi via radio possono essere ascoltati da chiunque si trovi all'interno dell'area di diffusione: questo servizio gestisce la crittografia dei frame attraverso l'algoritmo RC4;
9. transmission (trasmissione): è il servizio principale usato dalla STA 802.11 e viene invocato da ciascun messaggio all'interno della ESS; in sintesi consiste nello scambio di frame fra due stazioni a livello di MAC sublayer.

Verifichiamo le conoscenze

1. Completamento

1 La stazione base prende il nome di ..... nelle reti cellulari e di ..... nelle .....

2 Possiamo definire la seguente tassonomia delle reti wireless:

1 hop singolo, senza infrastruttura: .....

2 hop singolo con infrastruttura: .....

3 hop multipli, senza infrastruttura: .....

4 hop multipli con infrastruttura: .....

3 Con il termine Extended Service Set (ESS) si intende .....

4 Nella topologia ..... si realizzano comunicazioni peer-to-peer tra le stazioni (.....) che sono localizzate nella medesima area ..... e che costituiscono un insieme denominato .....

5 Nelle reti di tipo Infrastructure è presente una LAN di distribuzione denominata ....., che interconnette diversi ..... e trasporta a livello ..... le trame: può essere cablata oppure wireless, e in questo caso prende il nome di .....

6 I diversi BSS fisicamente possono essere locati all'interno di un ESS secondo diversi criteri:

- .....
- .....
- .....

7 Un Access Point è una entità che permette la ..... via ..... per le stazioni a esso associate.

8 L'Access Point è tipicamente un apparato con ridotte funzioni che può essere configurato per funzionare in due modalità, come ..... oppure come .....

2. Vero o falso

1 Lo standard 802.11 definisce con reti IBSS le reti *ad hoc*. V F

2 Lo standard 802.11 definisce con Reti ESS le reti *ad hoc*. V F

3 Nell'area BSA la funzione DCF deve essere presente in tutte le stazioni. V F

4 Le reti MANET sono dinamiche e di tipo concentrato. V F

5 Le reti MANET sono reti del tipo "multi hop". V F

6 Nella modalità infrastruttura, il BSS-ID corrisponde all'indirizzo MAC del punto di accesso. V F

7 Nella modalità infrastruttura il BSS-ID corrisponde al SSID. V F

8 L'802.11 gestisce il passaggio tra stazioni con un'unica modalità di transizioni. V F

9 Con lo scanning di tipo Active le AP trasmettono periodicamente beacon con il codice SSID. V F

10 Un AP di default viene configurato come "Root Access Point". V F

Esercitazioni di Laboratorio 1

ACCESS POINT LINKSYS CON PACKET TRACER

Rete Wi-Fi con Packet Tracer

Vogliamo realizzare una rete con Packet Tracer che utilizzi l'◀ Access Point ▶ Linksys WRT300N.

◀ Spesso identificato con l'acronimo AP, un Access Point è un dispositivo che raggruppa uno switch Wi-Fi e cablato, un router, oltre a un modem per la connessione a Internet. La funzionalità di Access Point viene spesso integrata nei più moderni router. ▶

Utilizzeremo l'Access Point disponibile con Packet Tracer: per fare questo possiamo posizionarci sui dispositivi wireless (Wireless Devices), quindi selezioniamo Linksys dall'elenco disponibile:

Zoom su...

PC CON SCHEDA WIRELESS

Vediamo come inserire anche dei PC che dispongono di schede di rete wireless. Posizioniamoci sui dispositivi Custom (Custom Made Devices):

Quindi scegliamo il dispositivo Generic Wireless PC:

Prima di tutto vediamo lo schema generale della rete, ai vari elementi vengono assegnate le seguenti configurazioni:

Un PC2

Indirizzo IP, subnet mask, DNS e Gateway assegnati dal DHCP Server

Due PC Wireless PC0 e PC1

Indirizzo IP, subnet mask, DNS e Gateway assegnati dal DHCP Server
SSID: MY_RETE
WPA2 PSK passphrase: password

Un Server DHCP

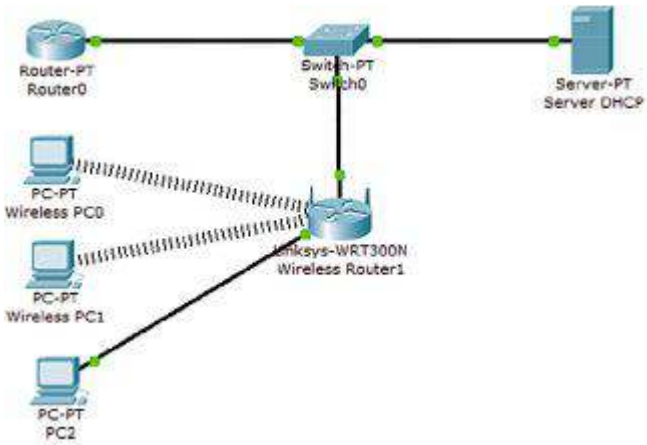
Indirizzo IP: 10.1.1.10/24
Gateway: 10.1.1.1
Server DNS: 10.1.1.10
DHCP: range (10.1.1.20 - 10.1.1.69),
DNS:
accesspoint.it (172.16.0.1)
gateway.it (10.1.1.1)
server.it (10.1.1.10)

Un Wireless Router 1 (Linksys-WRT300N)

Internet:
Indirizzo IP, subnet mask, DNS assegnati dal DHCP Server
LAN:
Indirizzo IP: 172.16.0.1/24
Wireless:
SSID: MY_RETE
WPA2 PSK passphrase: password
DHCP: Enabled
Start IP Address: 172.16.0.2
Maximum users: 50
Static DNS 1: 10.1.1.1

Un router Router0

Indirizzo IP: 10.1.1.1/24



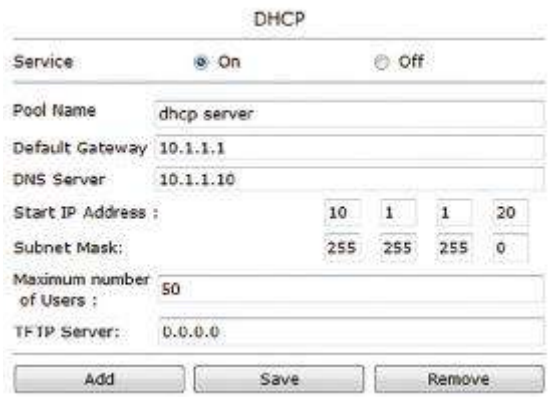
Configurare il Router

1. Facciamo clic sul Router0, quindi sulla interfaccia collegata con lo Switch0. Inseriamo l'indirizzo IP (10.1.1.1) e la Subnet Mask (255.255.255.0):

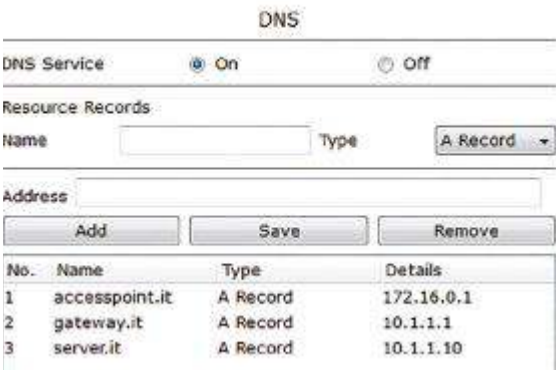
Configurare il server DHCP

1. Facciamo clic sul server e apriamo la scheda Config. In questa finestra inseriamo l'indirizzo del Gateway (10.1.1.1) e del DNS Server (10.1.1.10): ▶

2. Attiviamo il servizio DHCP, inserendo l'indirizzo del Default Gateway (10.1.1.1) e del DNS Server (10.1.1.10). Inseriamo poi il range di indirizzi che possono essere generati, digitandoli nelle caselle Start IP Address (10.1.1.20) e Subnet Mask (255.255.255.0). Quindi confermiamo con Add e Save: ▶

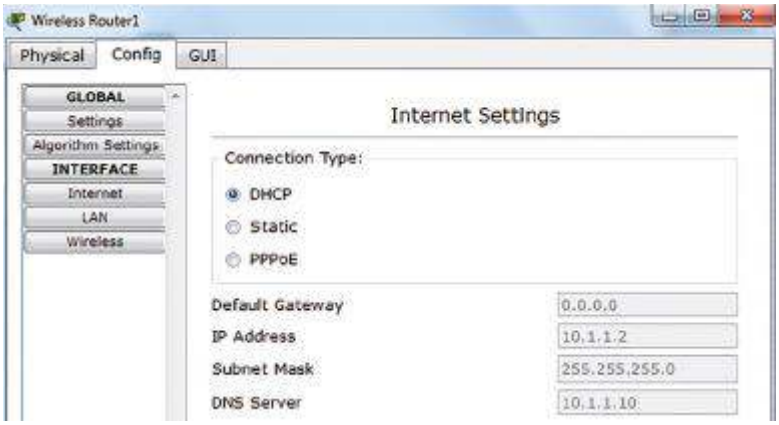


3. Passiamo a definire il servizio DNS, associando i nomi agli indirizzi IP indicati: ▶



Configurare il Wireless Router Linksys-WRT300N

1. Facciamo clic sull'icona del Wireless Router, quindi nella scheda Config, poi nell'interfaccia Internet. Come possiamo notare vengono assegnati dinamicamente (DHCP):

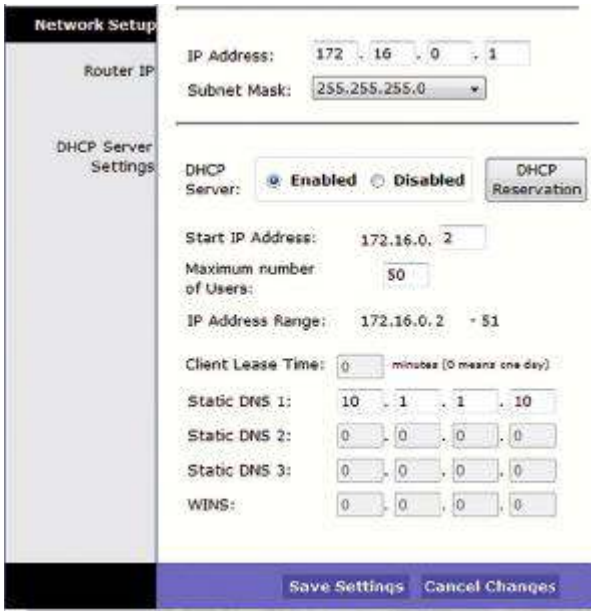


2. Passiamo al settaggio delle impostazioni LAN, cioè quelle coinvolte nella gestione dei dispositivi collegati via cavo. Inseriamo l'indirizzo IP 172.16.0.1, con la Subnet Mask indicata, ricordando che questo indirizzo è relativo alla interfaccia rivolta verso i PC collegati via cavo:

3. Passiamo al settaggio delle impostazioni dei dispositivi senza fili collegati (wireless). Assegniamo il nome alla rete Wi-Fi (SSID), in questo caso MY_RETE, quindi scegliamo la password WPA2-PSK (in questo caso password) e infine selezioniamo il tipo di criptaggio (AES).

4. Una volta stabilite queste informazioni passiamo alla configurazione delle impostazioni di rete, attiviamo il DHCP selezionando Enabled da DHCP Server. Assegniamo come indirizzo iniziale del range DHCP (Start IP Address) 172.16.0.2, quindi 50 come Maximum number of Users.

Infine assegniamo l'indirizzo 10.1.1.10 come server DNS (Static DNS 1). Confermiamo i dati salvandoli con Save Settings, posto nella parte bassa della finestra:



Configurare i singoli Host della rete

1. Facciamo clic sull'icona del Wireless PC (PC0), quindi nella scheda Config, poi nell'interfaccia Wireless. Inseriamo l'SSID della rete (MY_RETE), quindi la password (password) per abilitare la connessione attraverso WPA2-PSK. Attiviamo DHCP nella scheda IP Configuration, in tal modo riceveremo dall'Access Point sia l'indirizzo IP che la Subnet Mask.

2 Verifichiamo che nella sezione Global Settings sia stato attivata l'opzione DHCP. In tal modo sia l'indirizzo del Gateway che il DNS server verranno assegnati automaticamente:

Per il PC2 le operazioni sono più semplici in quanto non deve essere configurata la rete wireless.

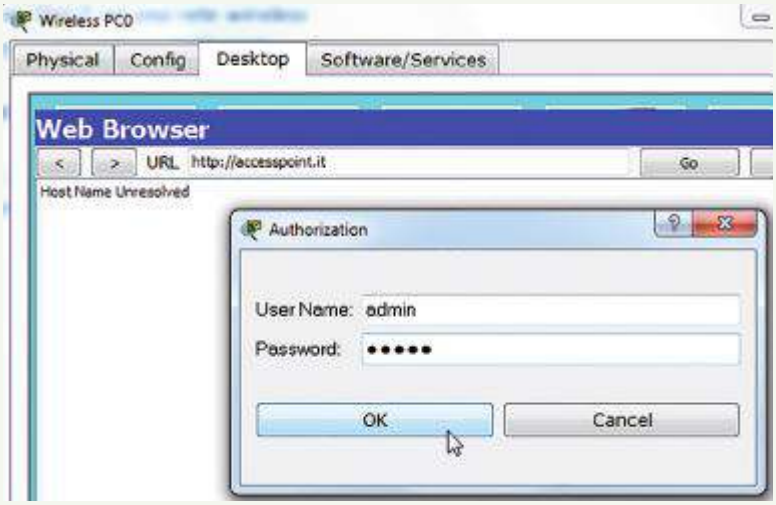
Prova adesso!

- Applicare un server DHCP a una rete wireless
- Utilizzare un Acess Point Linksys-WRT300N

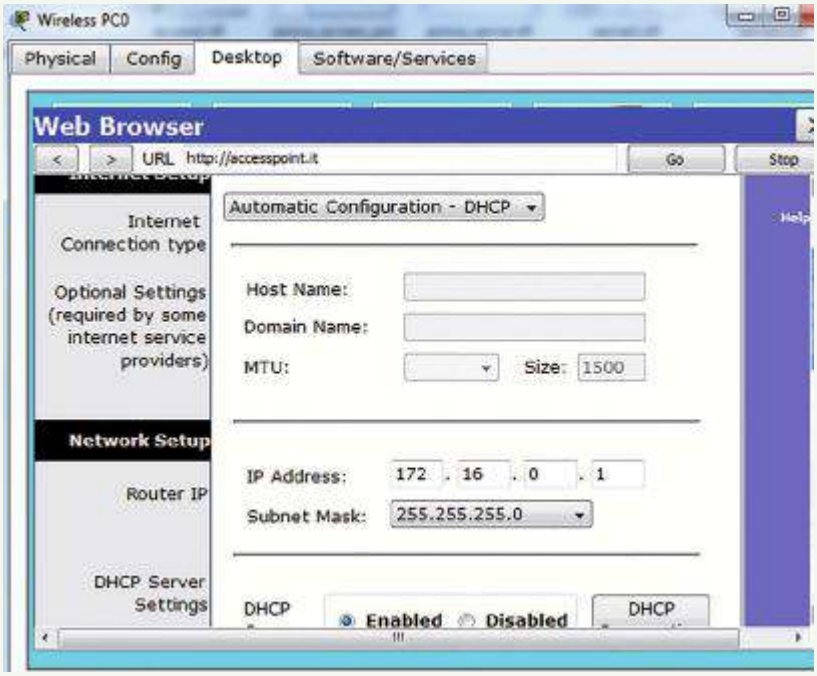
APRI L'ESEMPIO access_point.pkt

1 Verifica che si possa accedere al server aprendo la finestra Desktop, quindi Web Browser da uno dei PC presenti. A quel punto verifica che digitando nella casella URL l'indirizzo http://server.it, appaia la pagina Web disponibile sul server:

2 Verifica che si possa accedere all'Access Point Linksys, aprendo la finestra Desktop, quindi Web Browser da uno dei PC presenti. A quel punto verifica che digitando nella casella URL l'indirizzo http://accesspoint.it appaia la finestra di autenticazione per accedere al router wireless:



3 Dopo aver inserito le credenziali (admin, admin), possiamo notare che appare la pagina di configurazione dell'apparato Linksys:



Esercitazioni di Laboratorio 2

SERVER RADIUS CON PACKET TRACER

Server Radius

Vediamo come realizzare una rete che utilizzi un Server ◀ Radius ▶ per centralizzare le autenticazioni sui dispositivi di rete attraverso il protocollo AAA (Authentication, Authorization, Accounting).

◀ Radius (Remote Autentication Dial-In USer) è un protocollo che regola i meccanismi di autenticazione degli utenti alla rete LAN. L'architettura Radius prevede da una parte un server di accesso alla rete, comunemente indicato con la sigla NAS (Network Access Server) e dall'altra un server che si occupa invece di effettuare l'autenticazione dell'utente sulla rete, rappresentato dal Server Radius vero e proprio. ▶

Prima di tutto vediamo lo schema generale della rete, ai vari elementi vengono assegnate le seguenti configurazioni.

Un dispositivo wireless PC0
- Indirizzo IP, subnet mask e Gateway assegnati in DHCP dal Wireless Router1
- SSID: MY_RETE
- WPA2
- UserID: utente1
- Password: utente1
- Encryption Type: TKIP

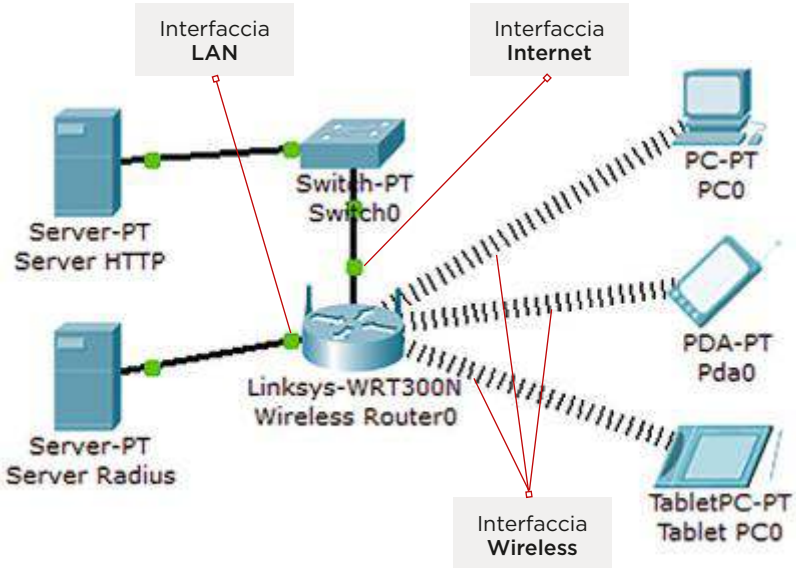
Un dispositivo wireless Pda0
- Indirizzo IP, subnet mask e Gateway assegnati in DHCP dal Wireless Router1
- SSID: MY_RETE
- WPA2
- UserID: utente2
- Password: utente2
- Encryption Type: TKIP

Un dispositivo wireless Tablet PC0
- Indirizzo IP, subnet mask e Gateway assegnati in DHCP dal Wireless Router1
- SSID: MY_RETE
- WPA2
- UserID: utente3
- Password: utente3
- Encryption Type: TKIP

Un Server HTTP
Indirizzo IP: 172.16.0.2/24
Servizio HTTP: Enable

Un Wireless Router 1 (Linksys-WRT300N)
Intenet:
Connection: Static
Indirizzo IP: 172.16.0.1/16
LAN:
Indirizzo IP: 192.168.0.1/16
Wireless:
SSID: MY_RETE
WPA2
Radius Server Settings:
IP Address: 192.168.0.50
Shared secret: secretpwd
DHCP: Enabled
Start IP Address: 192.168.0.100
Maximum users: 50

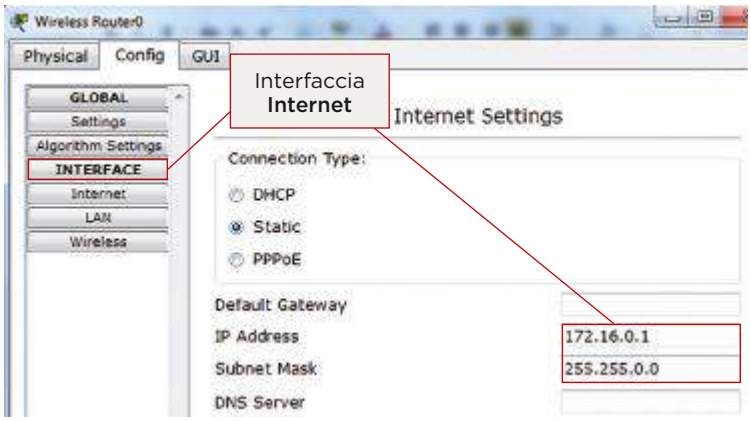
Un Server Radius
Indirizzo IP: 192.168.0.50/24
Servizio AAA
Network configuration:
Radius Port: 1645
Client Name: linksys
Client IP: 192.168.0.1/24
Key: secretpwd
Server Type: Radius
User Setup:
UserName: utente1, utente2, utente3
Password: utente1, utente2, utente3



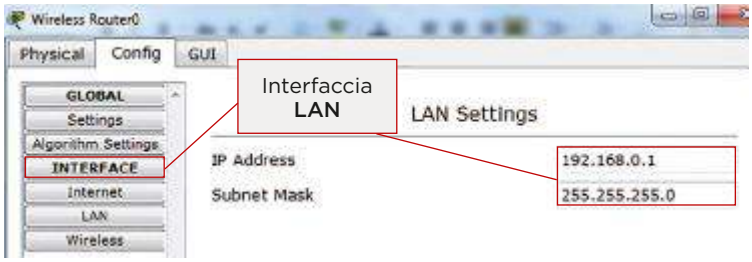
I paragrafi che seguono illustrano come realizzare la rete indicata.

Configurazione Wireless Router

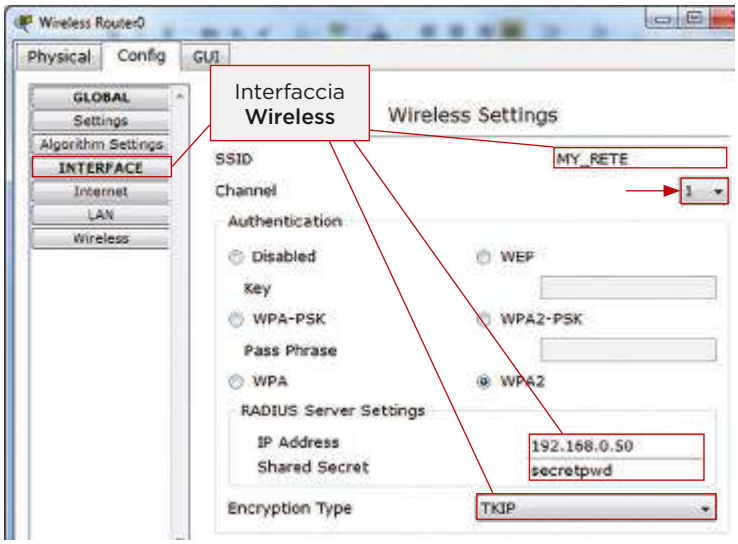
1. Per prima cosa, dopo aver collocato i vari componenti indicati nello schema precedente, passiamo alla configurazione del Wireless Router0. Facendo clic su di esso appare la consueta finestra nella quale andiamo a settare, nella scheda Config, le impostazioni di rete. Iniziamo a configurare l'interfaccia Internet. L'interfaccia associata verrà collegata al Server HTTP tramite uno Switch (Switch0); definiamo l'indirizzo statico su tale interfaccia 172.16.0.1/16:



2. Configuriamo l'interfaccia LAN, assegnando l'indirizzo statico, qui obbligatorio, 192.168.0.1/24:



3. Infine assegniamo all'interfaccia wireless le diverse configurazioni. L'identificativo SSID della rete (MY_RETE), quindi l'indirizzo IP e la password associata al Server Radius (192.168.0.50 e secretpwd) e il tipo di criptaggio (TKIP).

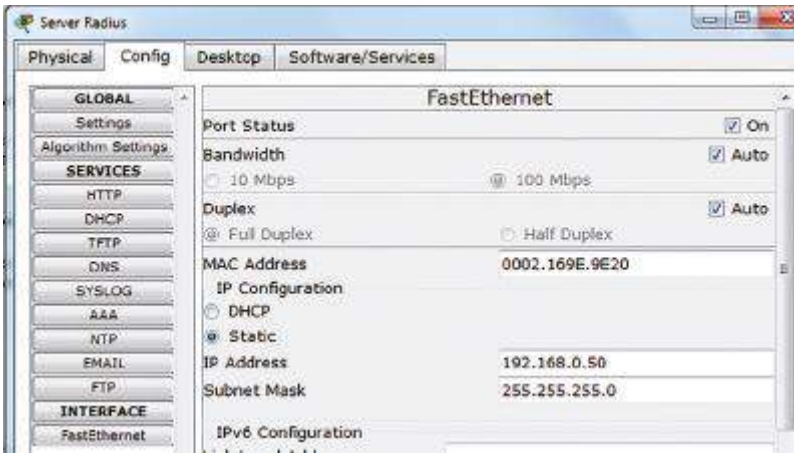


Non confondiamo l'autenticazione di tipo WPA2-PSK, con l'autenticazione WPA2: quest'ultima è infatti quella comunemente utilizzata per l'autenticazione senza fili sicura tramite Server Radius, mentre invece la WPA2-PSK viene utilizzata solo per l'accesso al Wireless Router.

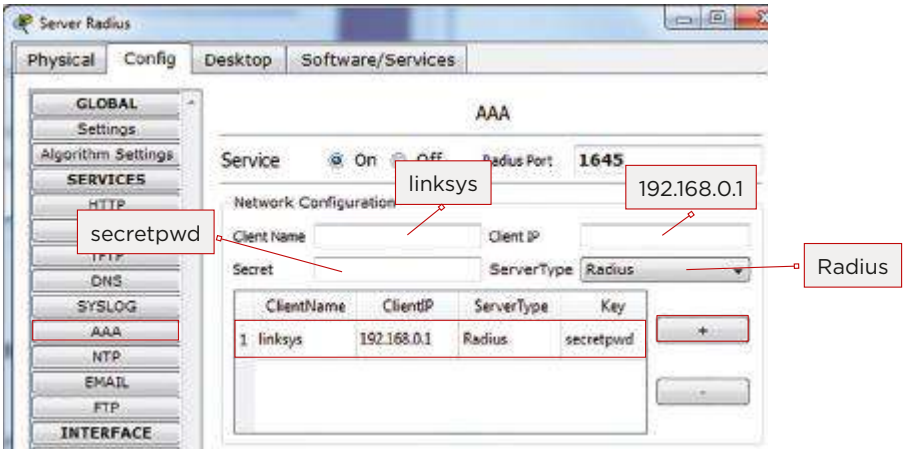
4 Facciamo clic sulla scheda GUI del Wireless Router per attivare gli indirizzi dinamici. Vogliamo generare gli indirizzi IP, secondo la modalità DHCP, con un range compreso tra 192.168.0.100 e 192.168.0.149, per i vari Host Wireless. Ricordiamo di salvare le impostazioni facendo clic su Save Settings, pulsante posto in basso nella finestra mostrata: ▶

Configurazione Server Radius

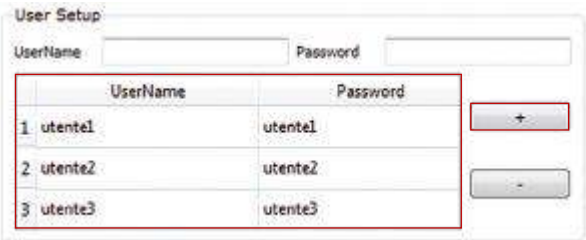
1 Passiamo alla definizione del Server Radius: lo colleghiamo alla porta LAN del Wireless Router, e assegniamo all'interfaccia l'indirizzo statico 192.168.0.50/24. Per fare questo, dopo aver fatto clic sul Server Radius, attiviamo la scheda Config, quindi il pulsante FastEthernet: ▶



2 Per definire le impostazioni di configurazione del server dobbiamo fare clic sul servizio AAA, quindi definiamo il servizio Radius assegnando il nome del client (è il nome dell'Access Point quindi linksys), quindi l'indirizzo IP (192.168.0.1), poi la password (secretpwd) e il tipo di server richiesto (Radius). Dopo aver digitato i dati facciamo clic sul pulsante + per aggiungere la configurazione: ▼

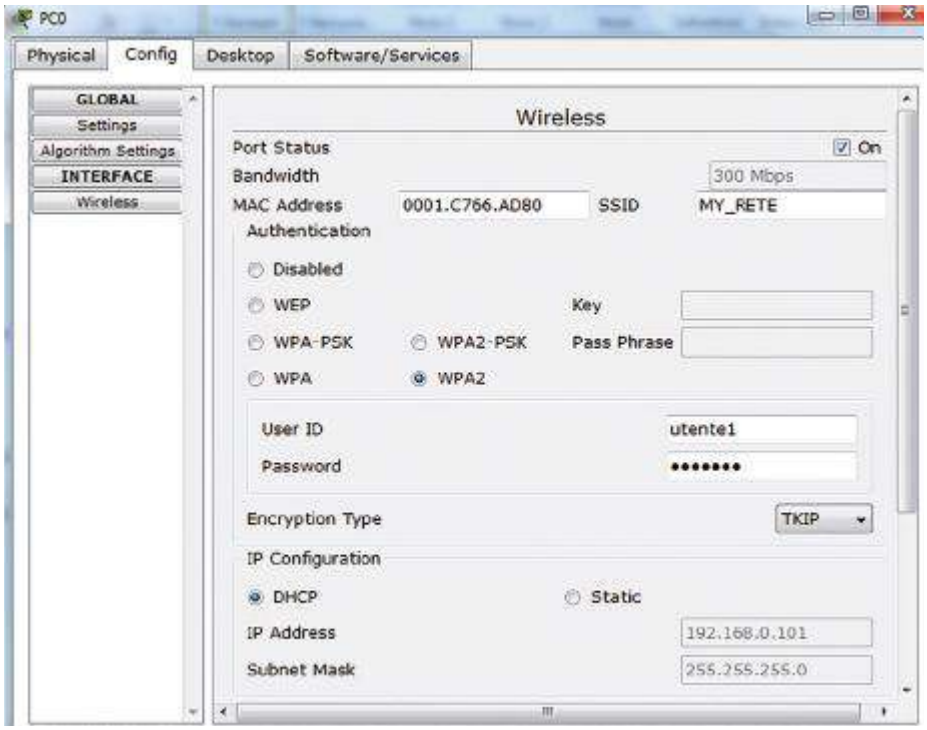


3 Nella stessa finestra dobbiamo anche aggiungere gli account che potranno accedere alla rete Wi-Fi. Ricordiamo che dopo aver digitato UserName e Password, dobbiamo fare clic su + per aggiungere l'account utente all'elenco: ▶



Configurazione client Wi-Fi

1 Per configurare i singoli client dobbiamo scrivere il nome utente, rappresentato dall'User ID (utente1) e la relativa Password nelle caselle riservate alla configurazione dell'autenticazione tramite WPA2, oltre all'Encryption Type (TKIP), come impostato sul Server Radius:



2 Ripetiamo la stessa operazione per tutti gli Host.

Prova adesso!

- Utilizzare un server Radius
- Gestire le autenticazioni Wi-Fi secondo il protocollo AAA

APRI IL FILE server_radius.pkt

1 Verifica che il sito Web presente sul server HTTP (172.16.0.2) sia raggiungibile dagli Host collegati tramite wireless.
2 Aggiungi un client Laptop PC e configuralo aggiungendo un nuovo utente e password AAA sul Server Radius. Verifica quanto effettuato testando la connessione.
3 Verifica che dal Server HTTP non sia raggiungibile l'Access Point, ma solo viceversa

Esercitazioni di Laboratorio 3

CONTROLLARE GLI ACCESSI WIRELESS CON WIRELESS NETWORK WATCHER

Le reti wireless hanno portato una rivoluzione importante nella nostra società e, per la loro comodità e semplicità di utilizzo, sono utilizzate praticamente in ogni rete locale e domestica.
Sono però anche poco sicure ed è possibile che intrusi utilizzino la nostra rete wireless, nel migliore dei casi solo per effettuare "gratuitamente" l'accesso a Internet, mentre nei casi più gravi per:

- violare la privacy: potrebbero accedere agli hard disk di rete copiando i file in essi memorizzati o danneggiandoli: inoltre potrebbero installare programmi keystroker, che leggono e memorizzano tutti i caratteri alfanumerici premuti sulla tastiera alla ricerca di password riservate;
- controllare il traffico di rete: potrebbe essere analizzato tutto il traffico di rete e le pagine Web visitate in tempo reale, con tanto di password che vengono inserite durante la navigazione;
- utilizzo della connessione a scopi illegali: la connessione potrebbe essere utilizzata per scaricare illegalmente musica, film coperti da copyright oppure per la condivisione di materiale pedopornografico.
- danneggiamento dei dati: potrebbero inserire nel sistema virus e malware.

Per accorgersi della presenza di intrusi si possono utilizzare software specifici che analizzano le connessioni delle reti wireless, come Wireless Network Watcher, un programma gratuito, semplice da utilizzare, che non necessita di installazione ma molto efficace nel rilevamento delle intrusioni.

> Il programma è scaricabile all'indirizzo http://www.nirsoft.net/network_tools.html oppure nella cartella materiali nella sezione del sito www.hoepliscuola.it riservata a questo volume.

Wireless Network Watcher è una piccola utility di soli 700 Kb che non richiede installazione e che analizza la rete wireless visualizzando l'elenco di tutti i computer e dispositivi che sono attualmente connessi alla rete: per ogni computer o dispositivo che è collegato alla rete vengono visualizzate le seguenti informazioni:

- indirizzo IP;
- indirizzo MAC;
- la società che ha prodotto la scheda di rete;
- il nome del computer (se presente).

È inoltre possibile esportare l'elenco di dispositivi collegati in file di testo html/xml/csv o copiare l'elenco negli Appunti e quindi incollare in Excel o altro foglio di calcolo.

Nell'esempio riportato di seguito il programma è stato mandato in esecuzione sul mio PC domestico, dove si può vedere che al server sono connessi 3 dispositivi wireless (due laptop e un iPhone).

Tra le opzioni disponibili, oltre alla possibilità di scegliere il formato di visualizzazione dell'indirizzo MAC, la più utile è quella che ci avvisa acusticamente quando nuovi dispositivi si connettono alla rete.

Se dall'analisi delle connessioni ci accorgiamo che qualche intruso si è introdotto abusivamente nella nostra rete, abbiamo alcune contromisure da prendere per proteggere meglio la rete wireless:

- **cambiare la password di amministrazione**: spesso non viene cambiata la password impostata dalla fabbrica e questo è il primo intervento che è doveroso effettuare: inserite una password lunga almeno 8 caratteri contenenti numeri e lettere, come descritto nella lezione 7 della UA3;
- **cambiare gli SSID della vostra rete**: modificare l'SSID della rete inserendo una passphrase complessa, che non faccia riferimenti personali;
- **disabilitare il broadcast SSID**: gli Access Point inviano i beacon per la sincronizzazione che contengono gli SSID; così facendo rendiamo la nostra rete invisibile;
- **spegnere l'Access Point quando non lo si utilizza**: questo è un semplice accorgimento che oltre a far risparmiare energia elettrica allontana i malintenzionati;
- **filtrare gli indirizzi MAC:** tutti gli AP permettono di inserire l'elenco dei MAC Andress autorizzati in modo da bloccare ogni altro dispositivo non riconosciuto. In questo modo, anche senza la presenza di una password, il vostro router apparirà sempre raggiungibile (rete Wi-Fi aperta), ma non lo sarà mai veramente perché funzionerà solo per i dispositivi segnalati al router con i MAC Andress;
- **cambiare la community di default di SNMP**: sugli AP nei quali è installato un SNMP è necessario configurare la community password in modo da evitare le intromissioni di qualche aggressore;

- non utilizzare come protezione solamente il WEP: dato che il WEP è un protocollo molto vulnerabile deve sempre essere usato assieme al WPA che è molto più sicuro e non vulnerabile;

- non utilizzare il DHCP: il DHCP permette la distribuzione automatica degli indirizzi IP a tutti i clienti che si collegano all'Access Point e in questo modo qualsiasi host può ottenere il vostro indirizzo IP e connettersi alla vostra rete: disabilitando il DHCP è necessario assegnare manualmente gli indirizzi IP ai computer che si vogliamo collegare alla rete, anche ai dispositivi wireless;

- limitare l'intensità del segnale wireless: le onde radio non si possono limitare in direzione e quindi bisogna collocare l'Access Point in modo da fornire un sufficiente collegamento solamente nella nostra zona che ci interessa e non all'esterno.

Per limitare in modo artigianale la potenza dell'AP è sufficiente porre sopra le antenne delle lattine di alluminio che possono ridurre il segnale anche del 20/30%.

Prova adesso!

Dopo aver installato Wireless Network Watcher, analizza i dispositivi connessi alla rete.
Quindi connetti il tuo laptop (oppure il telefonino) assegnandogli le credenziali necessarie per la connessione.
Successivamente individua gli indirizzi MAC degli host connessi e crea una Access List da inserire nel router.

Wearable computing

A term that refers to computer-powered devices or equipment that can be worn by a user, including clothing, watches, glasses, shoes and similar items. Wearable computing devices can range from providing very specific, limited features like heart rate monitoring and pedometer capabilities to advanced "smart" functions and features similar to those a smartphone or smartwatch offers.

Bluetooth

Bluetooth is defined as being a short-range radio technology (or wireless technology) aimed at simplifying communications among Internet devices and between devices and the Internet. It also aims to simplify data synchronization between Internet devices and other computers. Bluetooth products – that is products using Bluetooth technology – must be qualified and pass interoperability testing by the Bluetooth Special Interest Group prior to release.

Wi-Fi

Wi-Fi Alliance® is a global non-profit industry association of hundreds of leading companies devoted to seamless connectivity. With technology development, market building, and regulatory programs, Wi-Fi Alliance has enabled widespread adoption of Wi-Fi® worldwide. The Wi-Fi CERTIFIED™ program was launched in March 2000. It provides a widely-recognized designation of interoperability and quality, and it helps to ensure that Wi-Fi-enabled products deliver the best user experience. Wi-Fi Alliance has certified more than 15,000 products, encouraging the expanded use of Wi-Fi products and services in new and established markets. Wi-Fi®, Wi-Fi Alliance®, WMM®, Wi-Fi Protected Access® (WPA), the Wi-Fi CERTIFIED logo, the Wi-Fi logo, the Wi-Fi ZONE logo and the Wi-Fi Protected Setup logo are registered trademarks of Wi-Fi Alliance.

RADIUS

RADIUS (Remote Authentication Dial-In User Service) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point.

Wardriving

Peter Shipley coined the term wardriving, referring to the practice of deliberately searching a local area looking for Wi-Fi wireless network signals. Mr. Shipley pioneered the practice of using an automobile, a Global Positioning System (GPS), and a mounted antenna to identify unsecured wireless home networks.

System Requirements And Limitations

This utility works on Windows 2000, Windows XP, Windows Server 2003/2008, Windows Vista, Windows 7, and Windows 8. This utility can only scan a wireless network that you're currently connected to. It cannot scan other wireless networks. In rare cases, it's possible that Wireless Network Watcher won't detect the correct wireless network adapter, and then you should go to 'Advanced Options' window (F9), and manually choose the correct network adapter. Although this utility is officially designed for wireless networks, you can also use it to scan a small wired network.

UNITÀ DI APPRENDIMENTO

6

Modello client-server e distribuito per i servizi di rete

L1 **Le applicazioni e i sistemi distribuiti**
L2 **Architetture dei sistemi Web**
L3 **Amministrazione di una rete**
L4 **Active Directory**
L5 **Il troubleshooting**
L6 **La sicurezza della rete**

Esercitazioni di laboratorio

1 Installare Windows 2003 server; 2 Installare Active Directory; 3 Utility per la verifica della rete; 4 Gestire le policies con Active Directory; 5 Il monitoraggio di Windows server; 6 File Server e protezione NTFS; 7 Politiche di accesso remoto

Conoscenze

- Acquisire il concetto di elaborazione distribuita e architetture dei sistemi Web
- Conoscere l'evoluzione delle architetture informatiche
- Individuare le caratteristiche di server farm, partitioning e cloning
- Conoscere gli elementi che concorrono all'amministrazione di una rete
- Conoscere i domini e le relazioni di fiducia tra di essi
- Comprendere il ruolo di Active Directory nella gestione di un NOS
- Identificare e documentare i problemi di una rete attraverso il troubleshooting

Competenze

- Riconoscere i livelli di sicurezza da intraprendere
- Prendere i dovuti provvedimenti per la protezione dai principali tipi di attacco informatico
- Installare Windows server
- Utilizzare i servizi di directory di un sistema distribuito
- Installare Active Directory e gestire le policies di rete

Abilità

- Gestire i criteri di gruppo, i permessi NTFS e le condivisioni
- Utilizzare utilities per la verifica della rete, il monitoraggio del server e il disaster recover
- Saper configurare un file server e gestire le politiche di accesso remoto

AREA *digitale*

- Esercizi
- Architettura del Ministero delle Finanze
- Classificazione dei sistemi Web based
- Impostare i criteri di auditing

Soluzioni
Puoi scaricare il file anche da hoepliscuola.it

LEZIONE 1

Le applicazioni e i sistemi distribuiti

In questa lezione impareremo...

- il concetto di elaborazione distribuita
- l'evoluzione delle architetture informatiche
- la differenza tra server farm, partitioning e cloning
- le architetture dei sistemi informativi basate sul Web

Le applicazioni distribuite

Le ◀ applicazioni distribuite ▶ possono essere suddivise secondo tre livelli applicativi.

1. Il livello presentazione si occupa di gestire la logica di presentazione, quindi le modalità di interazione con l'utente: contiene le modalità di interfacciamento grafico e le modalità di rendering delle informazioni. Questo livello è anche denominato front end delle applicazioni.
2. Il livello della logica applicativa o logica di business si occupa delle funzioni da mettere a disposizione all'utente.
3. Infine il livello di logica di accesso ai dati si occupa della gestione dell'informazione, eventualmente con accesso alle basi di dati.

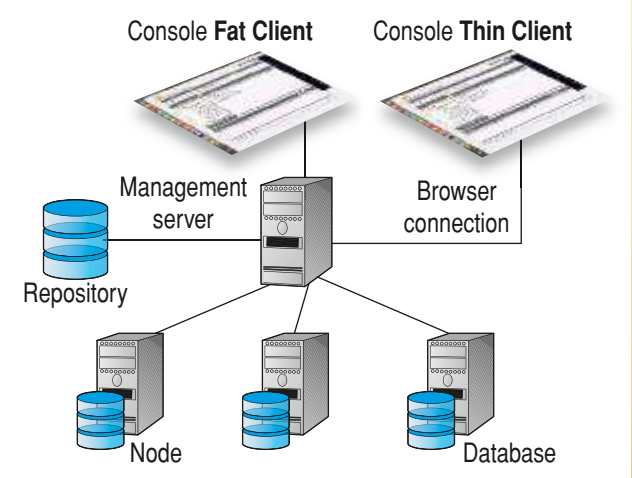
◀ Un'applicazione distribuita è costituita da due o più processi eseguiti, in parallelo, su macchine distinte connesse da una rete di comunicazione. I processi che costituiscono una applicazione distribuita cooperano sfruttando i servizi forniti dalla rete di comunicazione. ▶

Questi tre livelli applicativi (software) possono essere installati su vari livelli hardware, detti Tier, dove un livello rappresenta una macchina con differente capacità di elaborazione.

Un'applicazione può essere configurata come:

1. Single Tiered: i tre livelli sono ospitati su una singola macchina o host;
2. Two Tiered: i tre livelli sono divisi fra una macchina utente, che ospita il livello di presentazione, e la macchina server che ospita il livello di accesso ai dati; il livello di logica applicativa può risiedere sul lato utente o server o essere distribuito fra i due;
3. Three Tiered: i tre livelli risiedono ciascuno su una macchina dedicata, ovvero una stazione di lavoro utente (di tipo PC, in generale), un server per le applicazioni e un server per la gestione dei dati.

Possiamo parlare di configurazione fat client quando a livello utente (ad esempio il browser in ambiente Web) la logica applicativa si appoggia a quella di accesso ai dati, oppure di thin client quando a livello utente abbiamo solo il livello di presentazione, alleggerendo in tal modo le funzionalità della stazione utente.



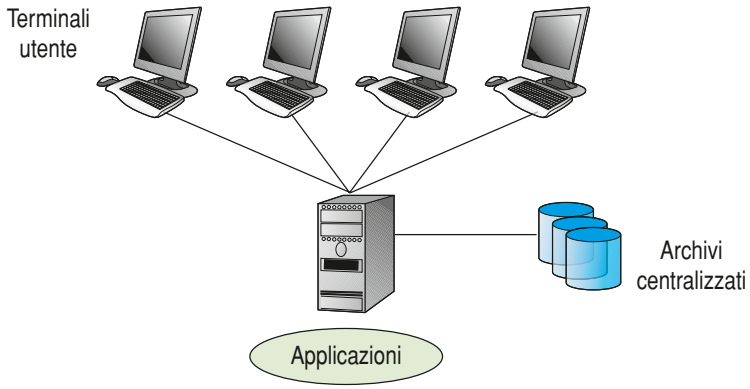
Il livello middleware che contiene la combinazione di accesso a basi dati distribuite in rete e di oggetti di controllo e di comunicazione viene anche chiamato back end. Per contro, il livello di presentazione è comunemente denominato front end.

AREA digitale
Architettura del Ministero delle Finanze

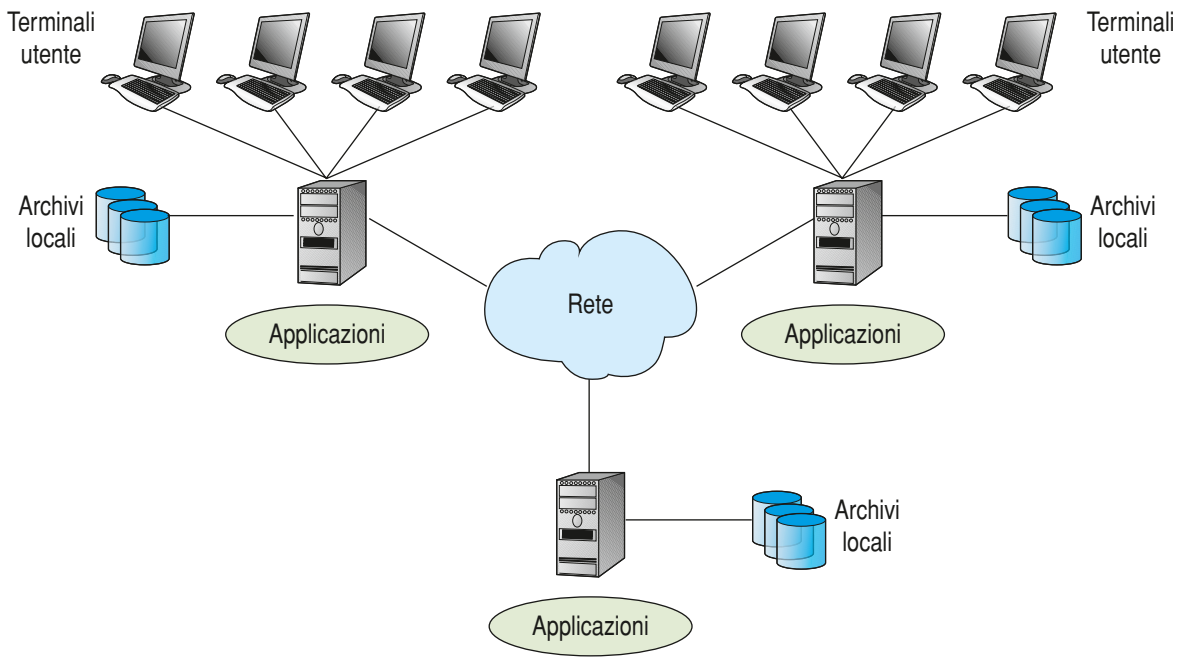
L'evoluzione delle architetture informatiche

L'architettura dei sistemi informatici indica l'insieme delle scelte tecniche e organizzative che influiscono sullo sviluppo e sull'utilizzo delle risorse tecnologiche di un sistema. Le architetture dei sistemi informatici si sono sviluppate ed evolute nel corso degli anni passando da sistemi centralizzati a ◀ sistemi distribuiti ▶, maggiormente rispondenti alle necessità di decentralizzazione e di cooperazione delle moderne organizzazioni.
Parliamo di sistema informatico centralizzato quando i dati e le applicazioni risiedono in un unico nodo elaborativo.

◀ I sistemi distribuiti sono formati da un insieme di applicazioni logicamente indipendenti che collaborano per il perseguimento di obiettivi comuni attraverso una infrastruttura di comunicazione hardware e software. ▶



Un sistema informatico distribuito è quello che realizza almeno una delle seguenti situazioni:
- le applicazioni, fra loro cooperanti, risiedono su più nodi elaborativi (elaborazione distribuita);
- il patrimonio informativo, unitario, è ospitato su più nodi elaborativi (base di dati distribuita).



In termini generali, quindi, un sistema distribuito è costituito da un insieme d'applicazioni logicamente indipendenti che collaborano per il perseguimento d'obiettivi comuni attraverso un'infrastruttura di comunicazione hardware e software.

Server farm

I tier fisici analizzati in precedenza possono essere realizzati anche come server farm che viene gestita dagli altri livelli come se fosse un'unica risorsa. Una server farm è formata da un insieme di elaboratori che condividono le applicazioni e i dati.
Le server farm possono essere realizzate secondo due principi progettuali:

- cloning (clonazione);
- partitioning (partizionamento).

Cloning

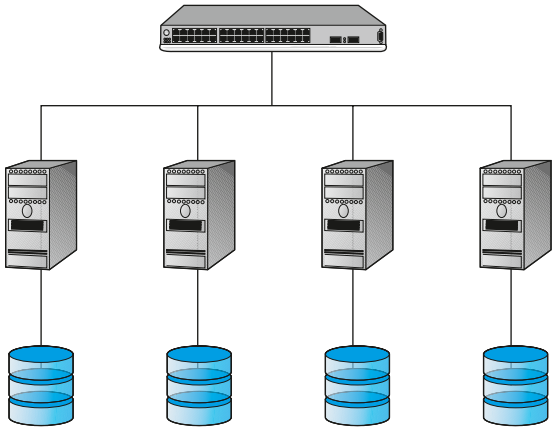
Nel primo caso, su ogni nodo che la compone vengono installate le stesse applicazioni software e gli stessi dati formando in tal modo dei cloni. Le richieste vengono poi inviate ai vari cloni attraverso un sistema di ◀ load-balancing ▶.

◀ Il bilanciamento del carico è una tecnica che distribuisce il carico di elaborazione tra diversi server. In questo modo vengono migliorate la scalabilità e l'affidabilità dell'architettura nel suo complesso. Se ad esempio giungono 20 richieste per una pagina Web su un cluster di 4 server, alle prime 5 risponderà il primo server, alle altre 5 il secondo e così via. La scalabilità deriva dal fatto che, nel caso sia necessario, si possono aggiungere nuovi server al cluster, mentre la maggiore affidabilità deriva dal fatto che la rottura di uno dei server non compromette la fornitura del servizio che in tal caso diventa anche fault tolerance. Infatti i sistemi di load balancing integrano sistemi di monitoraggio che escludono automaticamente dal cluster i server non raggiungibili evitando in tal modo di rispondere in modo errato a una richiesta dei client. ▶

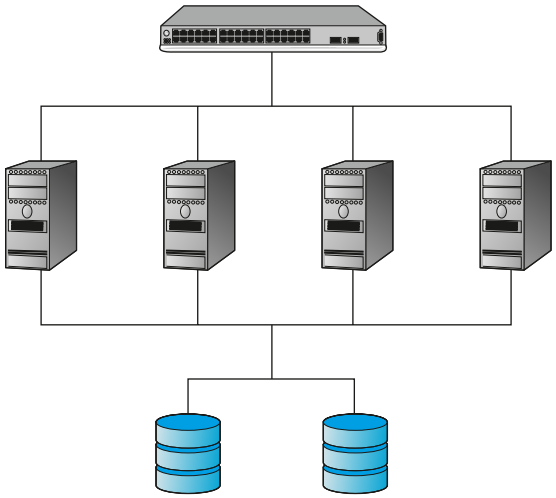
Un insieme di cloni dedicati allo svolgimento di un particolare servizio è detto RACS (Reliable Array of Cloned Services), in cui se un clone subisce un guasto, un altro nodo può continuare a erogare quel servizio.

I RACS si possono presentare in due configurazioni:
- shared nothing;
- shared disk.

Nella prima configurazione i dati memorizzati sono replicati su ogni clone e risiedono in un disco fisso locale a ogni clone; quindi, un aggiornamento di dati deve essere applicato a ognuno dei cloni. Questa configurazione presenta ottime prestazioni per applicazioni di tipo read-only, quali ad esempio l'accesso a pagine statiche o il download di file o immagini dai Web server. ▶

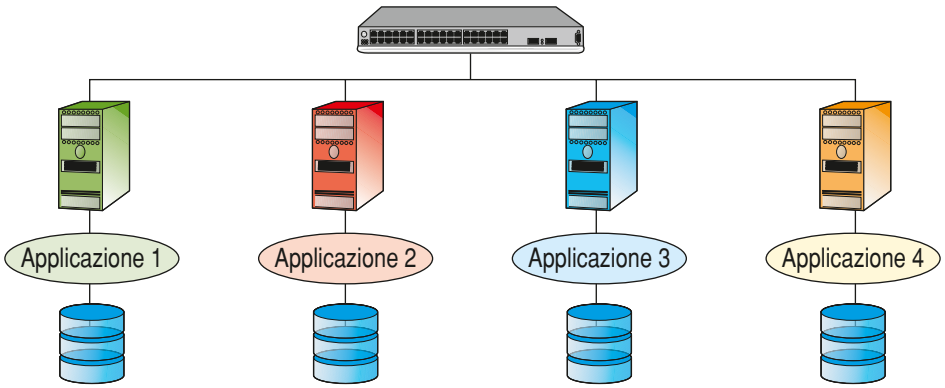


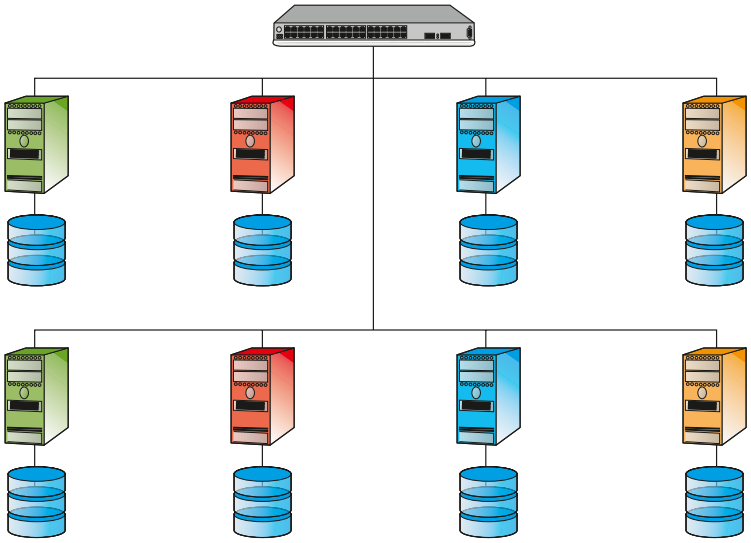
Nella seconda configurazione, detta anche cluster, i cloni condividono un server di memorizzazione che gestisce i dischi fissi, come possiamo vedere dall'immagine seguente: ▶



Partitioning

La tecnica di partizionamento prevede viceversa la duplicazione dell'hardware e del software ma non dei dati, che invece vengono ripartiti tra i nodi. Ogni nodo svolge quindi una funzione specializzata; ad esempio il sistema Web di vendite di un'azienda può essere suddiviso per tipologie di clienti o per linee di prodotto e ognuna è gestita da un nodo.





Il partizionamento è trasparente alle applicazioni, le richieste vengono inviate alla partizione che possiede i dati rilevanti. Se viene implementato ad esempio un partizionamento per tipi di merce (merce1, merce2 ecc.), le richieste di accesso alla tipologia di merce1 vengono instradate al server che è in grado di accedere ai dati della merce richiesta. Tuttavia i dati sono memorizzati su un singolo server, questo significa che in caso di guasto la parte di servizio da esso gestita non risulta più accessibile. Questa caratteristica è nota come proprietà di graceful degradation (degrado parziale) dei sistemi distribuiti: a differenza dei sistemi centralizzati, in caso di malfunzionamento non tutto il sistema risulta inaccessibile, ma solo alcune funzionalità non risultano più disponibili. Per risolvere il problema di indisponibilità di alcune funzionalità applicative in caso di guasto, si impiega spesso la clonazione dei singoli server che costituiscono la partizione, creando in tale modo dei pack. Si parla allora di RAPS (Reliable Array of Partitioned Service) che rappresenta una soluzione che garantisce sia scalabilità che disponibilità del servizio.

Modelli di sistemi distribuiti: Windows

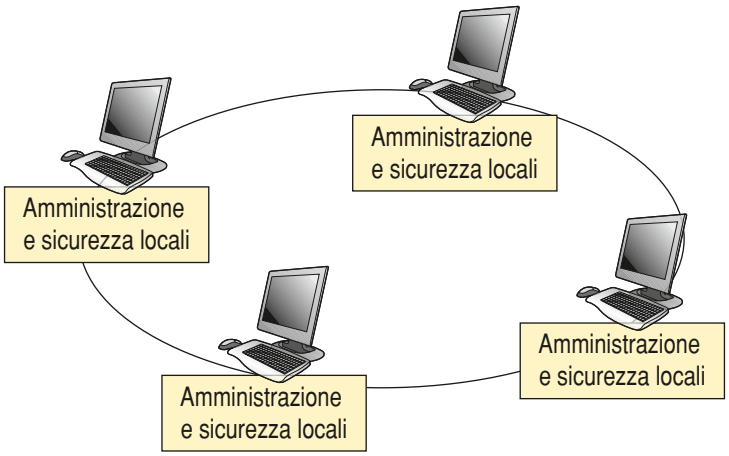
Windows consente la gestione di due modelli di organizzazione di una rete di calcolatori, per offrire servizi multipiattaforma e operazioni sicure, che possono essere così sintetizzati:

- modello a Workgroup;
- modello a Dominio.

Il modello a workgroup

Ogni host viene gestito autonomamente:

- le politiche di sicurezza e di accesso sono di difficile impostazione;
- i costi di gestione sono molto alti.



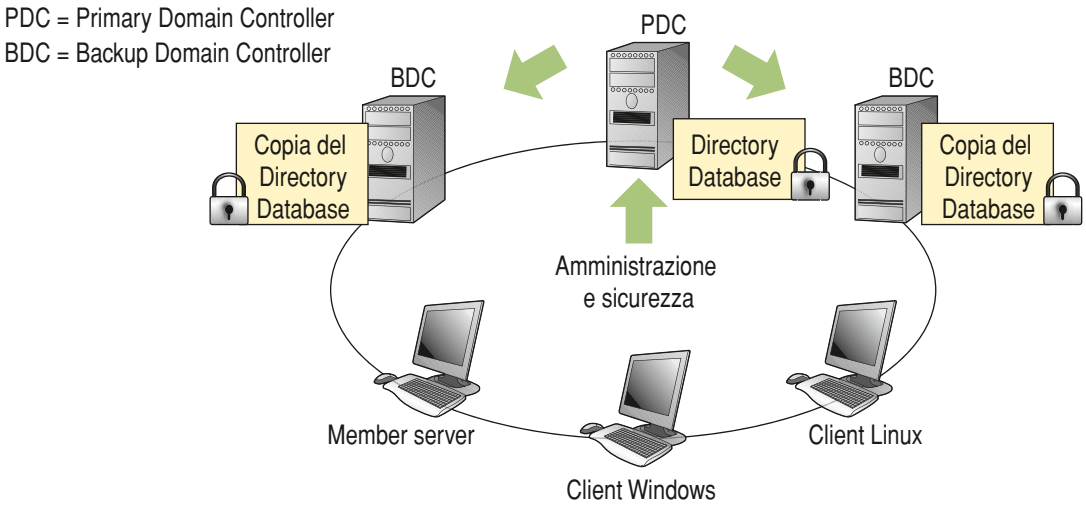
Il modello a workgroup è un raggruppamento logico di computer che consente la localizzazione di risorse nella rete (stampanti, file, CD-ROM, modem) in quanto rende possibile la visualizzazione delle directory condivise di ogni altro membro del workgroup tramite servizi di browsing. Inoltre ogni macchina in esso funziona come server stand-alone per cui possiede il proprio database contenente informazioni su account utenti e gruppi e non divide tali informazioni con gli altri computer del workgroup. L'amministratore (proprietario) del computer decide quali risorse condividere nel workgroup e con chi.

Il modello a dominio

In questo modello la rete possiede una gestione centralizzata degli utenti e delle relative politiche di sicurezza. Un dominio è un gruppo di client e server che condividono una politica di sicurezza e il database degli utenti. I server vengono di norma suddivisi tra:

- PDC server;
- BDC server;
- Stand alone server.

Il PDC (Primary Domain Controller) mantiene il database di directory con le informazioni di account per il dominio, è il server primario che tratta l'autenticazione degli utenti.
Il BDC (Backup Domain Controller) mantiene copie di backup del database di directory del dominio che non possono essere manipolate direttamente. Trattano inoltre l'autenticazione degli utenti se il PDC non è disponibile. La memorizzazione di più copie del database di directory consente l'aumento del grado di fault tolerance nella struttura di rete: maggiore è il numero di BDC e maggiore è l'efficienza della struttura di rete.
Lo stand alone server non memorizza copie del database di directory del dominio e memorizza e gestisce un proprio database di directory.



Un dominio può essere formato da gruppi di sistemi considerati come una sola situazione circoscritta in termini di sicurezza. Organizzano le risorse localizzate in diversi sistemi in un unico complesso amministrativo comportando una amministrazione centralizzata delle risorse del dominio e la possibilità per un utente di sottoporsi a una unica procedura di logon per avere accesso a tutte le risorse nel dominio.

AREA digitale
Classificazione dei sistemi Web based

Verifichiamo le conoscenze

1. Completamento

1 I ..... sono formati da un insieme di applicazioni ..... che collaborano attraverso una infrastruttura di comunicazione hardware e software.

2 Un'applicazione distribuita è una applicazione costituita da ..... che vengono eseguiti in parallelo.

3 I processi che costituiscono un'applicazione distribuita cooperano sfruttando i servizi forniti dalla .....

4 In un'applicazione single tiered i tre livelli sono ospitati .....

5 RACS rappresenta un insieme di ..... dedicati allo svolgimento di un particolare servizio, se uno subisce un guasto, un altro può continuare a erogare quel servizio.

6 Le applicazioni distribuite possono essere suddivise secondo tre livelli applicativi:

- .....
- .....
- .....

7 Le server farm possono essere realizzate secondo due principi progettuali:

- .....
- .....

8 Si definisce una configurazione ..... quando a livello utente la logica applicativa si appoggia a quella di accesso ai dati, oppure di ..... quando a livello utente abbiamo solo il livello di presentazione.

9 I RACS si possono presentare in due configurazioni:

- .....
- .....

10 Windows ammette due modelli di organizzazione di rete:

- .....
- .....

11 Nella configurazione shared disk i ..... condividono un server di memorizzazione che gestisce i .....

2. Vero o falso

1 Il livello di logica di accesso ai dati si occupa delle funzioni da mettere a disposizione dell'utente. V F

2 In un'applicazione Two Tiered i tre livelli sono divisi fra una macchina utente, che ospita il livello di presentazione, e la macchina server che ospita il livello di accesso ai dati. V F

3 Il livello di presentazione è comunemente denominato back end. V F

4 Una server farm è formata da un insieme di elaboratori che condividono le applicazioni e i dati. V F

5 Il load-balancing è una tecnica che distribuisce il carico di elaborazione tra diversi server. V F

6 Nel modello a workgroup la rete possiede una gestione centralizzata degli utenti e delle relative politiche di sicurezza. V F

LEZIONE 2

Architetture dei sistemi Web

In questa lezione impareremo...

- a conoscere le principali architetture dei sistemi Web
- a riconoscere gli elementi e le categorie delle architetture Web

Architetture dei sistemi Web

Gli elementi essenziali di un moderno sistema Web sono:

- il Web server, che si occupa della gestione delle richieste HTTP provenienti da Internet o dalla Intranet aziendale;
- lo Script engine, un processo che esegue script per la generazione di pagine HTML dinamiche;
- l'Application server, che assume il ruolo di middle tier e implementa la logica di business dell'applicazione Web;
- il DBMS server, che si occupa della gestione dei dati.

Il Web server si colloca fisicamente tra l'utente che accede al sistema attraverso il browser (tier applicativo) e il sistema informativo aziendale. Il Web server si occupa della presentazione delle informazioni verso i client e in particolare restituisce direttamente ai client che ne hanno fatto richiesta pagine HTML statiche o oggetti statici, come ad esempio immagini o file di altra natura. Quando è necessario generare una pagina dinamica, il Web server interagisce con lo ◀ Script engine ▶.

◀ Lo Script engine è un processo che genera una pagina dinamica, ad esempio in Java lo Script Engine è un Servlet Engine, un processo che esegue nel proprio spazio di indirizzamento una Servlet. ▶

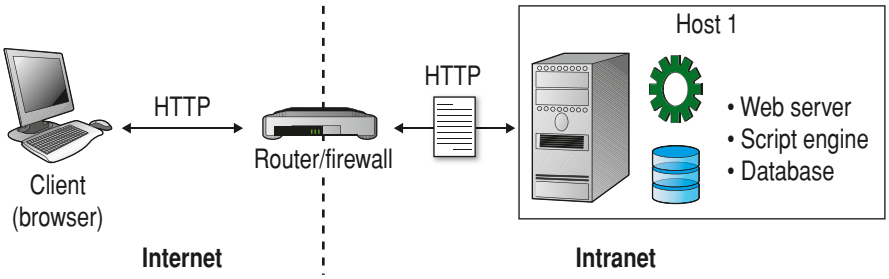
Lo Script engine genera pagine dinamiche interagendo con l'Application server o con il DBMS server. Le pagine dinamiche vengono poi restituite al Web server che le inoltrerà successivamente all'utente che ne ha fatto richiesta.

L'Application server svolge il ruolo di middle tier, implementando la logica di business dell'applicazione e in alcuni casi svolge il ruolo di contenitore di oggetti, consentendo l'esecuzione di un oggetto distribuito, come ad esempio Apache Tomcat, Microsoft.NET. Infine, come nei sistemi distribuiti tradizionali, il DBMS si occupa dell'accesso e della gestione dei dati aziendali.

Riassumendo, l'architettura di un sistema Web stabilisce:
- il numero di tier fisici del sistema, ovvero quali elementi (Web server, Script engine ecc.) devono essere installati su macchine fisiche separate;
- quante macchine devono essere introdotte a ogni tier fisico;
- come collegare tra di loro le diverse macchine.

Configurazione con due tier e unico host

Questa configurazione utilizza una sola macchina fisica che supporta l'esecuzione di Web server, script engine e DBMS.

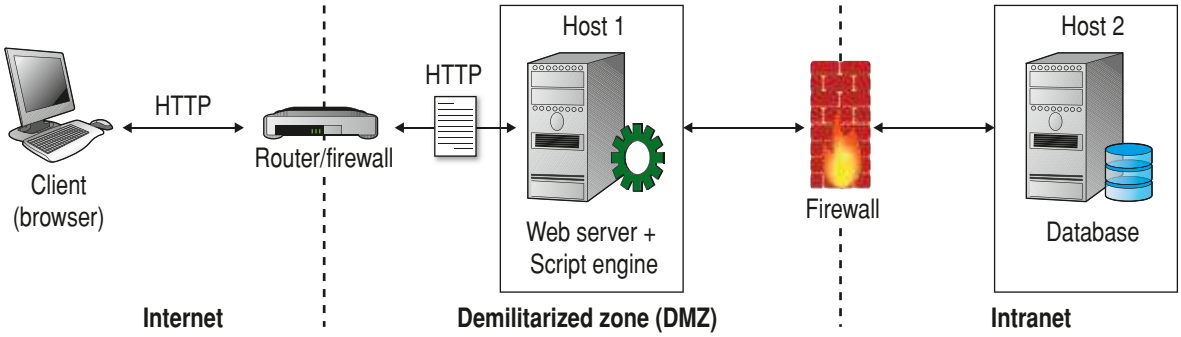


Questa configurazione prevede che il Web server richiami uno script esterno per la generazione della pagina Web dinamica. Si tratta di una configurazione che limita le prestazioni del sistema, si vengono a creare numerosi overhead dovuti alla continua attivazione/disattivazione dei processi e apertura/chiusura delle connessioni al DBMS.

L'unico vantaggio di questa configurazione è legato alla semplicità di installazione e manutenzione in quanto realizzato su di un solo host che ospita il Web server, lo script engine e il DBMS. Il sistema risulta tuttavia poco affidabile in quanto il malfunzionamento di un unico componente bloccherebbe l'accesso all'intero sistema. Inoltre il sistema è poco sicuro: qualora un intruso superi il firewall, il sistema diventa interamente accessibile. Tuttavia l'aspetto più critico dal punto di vista delle prestazioni risiede nel fatto che Web server e DBMS sono due processi che richiedono molte risorse sia in termini di utilizzo della memoria RAM che di CPU. La scalabilità del sistema inoltre è limitata alla possibilità di upgrade della singola macchina (incremento RAM, sostituzione CPU o dischi ecc.). Per il principio di downsizing, il costo del sistema risulta basso solo se non è richiesto hardware ad alte prestazioni.

Configurazione con tre tier e dual host

In questa configurazione Web server e Script engine sono ospitati su una stessa macchina, mentre il DBMS è eseguito su una macchina dedicata.



Inoltre, viene installato un secondo firewall che introduce un secondo dominio di sicurezza a protezione del DBMS.

La rete a cui risulta collegato il Web server viene detta DMZ (Demilitarized Zone), che consiste in un segmento, o insieme di segmenti, della rete localizzati tra reti protette e non protette. Questo argomento è già stato discusso in precedenza.

Il secondo livello di firewall garantisce una migliore protezione ai dati aziendali: infatti, anche se un intruso è in grado di scardinare il primo livello di firewall (Web server), deve necessariamente perdere altro tempo per superare il secondo ostacolo rappresentato dal secondo firewall (DBMS). Durante questo tempo il sistema può utilizzare la tecnica ◀ IDS (Intrusion Detection) ▶ per rilevare e bloccare l'attacco.

◀ Per spiegare cos'è e come funziona nel dettaglio la tecnica IDS non basterebbe un intero volume, tuttavia cercheremo di darne almeno una definizione. Si tratta di un dispositivo software e/o hardware utilizzato per identificare o prevenire accessi non autorizzati ai computer o alle reti locali. Le intrusioni rilevate possono essere quelle prodotte da cracker esperti, da tool automatici o da utenti inesperti che utilizzano programmi semiautomatici. I metodi tramite i quali questi software operano sono quelli di analizzare il sistema al fine di verificare comportamenti non usuali da parte della risorsa monitorata. Le analisi si concentrano su:

- file di log;
- integrità dei file locali (modifiche sospette possono essere sintomo di una avvenuta irruzione);
- pacchetti destinati all'host, sia per reagire a pattern di attacco noti che per accorgersi di un port scan remoto, generalmente prologo di un tentativo di intrusione.

Le tecniche di rilevamento si basano sui dati raccolti dai sensori che riescono a scoprire se ci sono delle anomalie. Queste tecniche possono essere divise in due categorie:

- Misuse Detection;
- Anomaly Detection.

La prima identifica le intrusioni ricercando pattern nel traffico di rete o nei dati generati dalle applicazioni (log analisys) e codifica e confronta una serie di segni caratteristici (signature action) delle varie tipologie di scenari di intrusione conosciute, come ad esempio cambi di proprietà di un file oppure stringhe di caratteri inviate a un server.
La seconda invece è stata ideata per sopperire ai difetti della precedente tecnica che non era in grado di rispondere a nuovi pattern o stringhe di attacco. L'anomaly detection è un sistema ad auto apprendimento attraverso cui viene analizzato il sistema alla ricerca di anomalie, creando nel contempo il profilo ottimale. Il profilo ottimale del sistema viene effettuato durante il normale funzionamento attraverso misure statistiche ed euristiche dello stesso, come ad esempio l›utilizzo della CPU di una macchina, il traffico dati di un particolare nodo ecc. Quindi stila una serie di regole che definiscono lo stato normale del sistema, confrontandolo via via con le nuove situazioni in cui il sistema si trova a funzionare. ▶

Inoltre, il dimensionamento della macchina dedicata all'esecuzione di Web server e Script engine e del server dedicato all'esecuzione del DBMS risulta meno critico. Rispetto alla configurazione precedente, la scalabilità del sistema è maggiore potendo intervenire separatamente su tier intermedio e data tier. Resta comunque critica la disponibilità del sistema, dato che è sufficiente il guasto di un componente per bloccare l'intero sistema.

Configurazione con tre tier e server farm

Per ottenere un sistema che migliori le caratteristiche di disponibilità, scalabilità e prestazioni è necessario duplicare i due componenti più critici del sistema perché sottoposti a continui accessi: Web server e/o Script engine. La duplicazione o replicazione è applicabile a ogni livello introducendo server farm in configurazione RACS o RAPS (viste in precedenza). In pratica per l'esecuzione del Web

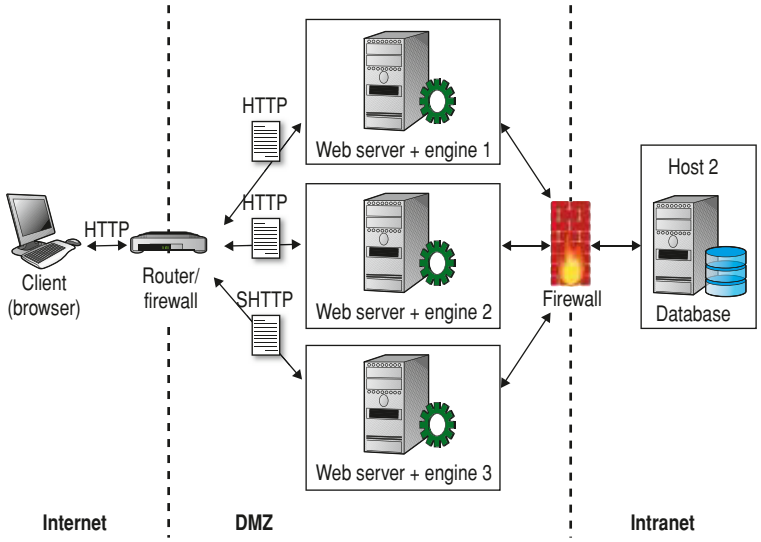
server, dello Script engine e dell'Application server vengono introdotte server farm in configurazioni RACS shared nothing. Invece per il DBMS vengono replicati schemi shared disk che si appoggiano su un server di memorizzazione o che sfruttano tecnologie moderne di ◀ storage networking ▶.

◀ Si tratta di sistemi SAN (Storage Area Network) e NAS (Network Attached Storage) che consentono a più server di condividere un insieme di dischi attraverso reti ottiche ad alta velocità. I sistemi NAS archiviano i dati su disco rigido in configurazione RAID, con un proprio indirizzo IP. Il vantaggio dei dispositivi NAS è che anche in ambienti in cui ci sono diversi server con sistemi operativi differenti, l'archiviazione, la gestione e il backup dei dati può essere centralizzata ed è inoltre facile aggiungere ulteriore spazio di archiviazione.
I sistemi SAN sono formati da una rete ad altissima velocità (dell'ordine dei Gigabit/s) costituita da una serie di dispositivi di memorizzazione di massa condivisi. Un dispositivo è una macchina che può essere composta da uno o più dischi per contenere dati. I protocolli attualmente più diffusi per l'utilizzo in questo ambito sono FC (FibreChannel) e iSCSI (Internet SCSI). Lo scopo della creazione di una SAN è principalmente quello di lavorare in modo che tutti i dispositivi di memorizzazione siano disponibili a qualsiasi server della rete LAN di cui la SAN in questione fa parte; una SAN può essere anche condivisa fra più reti interconnesse, anche di natura diversa: in tal caso uno dei server locali fa da ponte fra i dati memorizzati e gli utenti finali. Il vantaggio di simili architetture risiede nella concentrazione di tutta la potenza di calcolo messa a disposizione dei server esclusivamente per far girare applicazioni, delegando il compito della distribuzione dei dati fra i vari server e fra i server e i clients alle apparecchiature della SAN. ▶

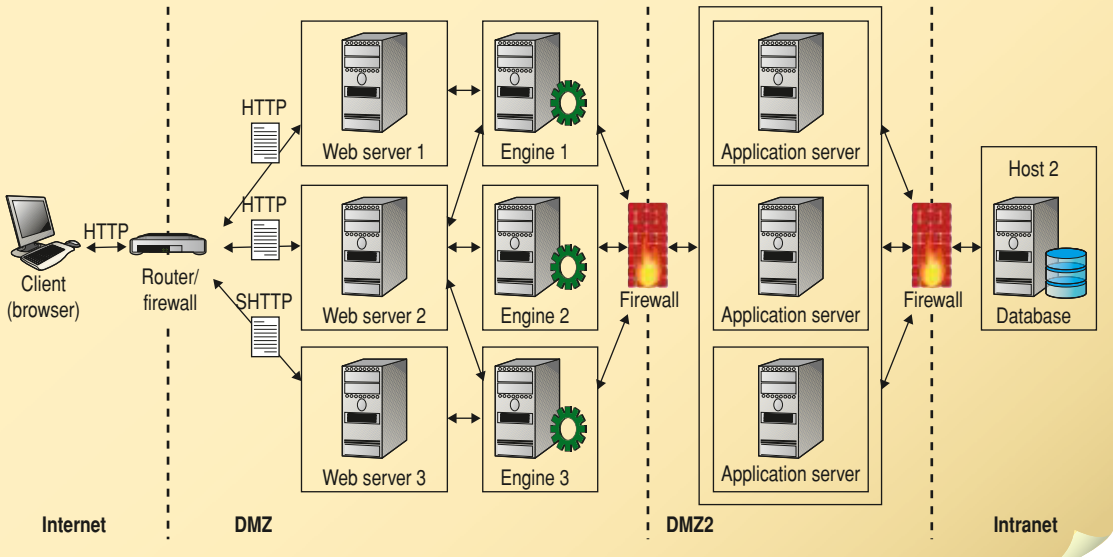
La replicazione dei componenti critici migliora la disponibilità del sistema, poiché, se cade uno dei processi, il suo carico di lavoro viene distribuito sugli altri processi in esecuzione e il sistema continua a erogare il proprio servizio. Inoltre, migliora la scalabilità del sistema dato che, se si presenta un collo di bottiglia a un qualsiasi livello è possibile introdurre nuove istanze di processi e nuove macchine server là dove risulta necessario, senza avere il limite della possibilità di upgrade di una singola macchina. La replicazione infine consente di migliorare le prestazioni poiché il carico viene distribuito dai load balancer in modo bilanciato sui server attivi.
Per quanto riguarda il Web server, la richiesta di una pagina Web può essere eseguita in parallelo dalle varie macchine che costituiscono la server farm, riducendo i tempi di risposta del sistema.
La replicazione può essere attuata in modo semplice per applicazioni stateless; risulta invece più problematica quando è necessario mantenere lo stato delle sessioni utenti. Le soluzioni che possono essere adottate consistono nell'introdurre load balancer evoluti che indirizzano le richieste provenienti da uno stesso client allo stesso server che mantiene lo stato della sessione. I load balancer devono essere dotati di una certa "intelligenza" e operano in generale a livello 7 dello stack ISO/OSI. Infatti, il semplice indirizzo IP del client può non essere sufficiente per discriminare l'utente collegato al sistema, dato che tutti gli utenti di una stessa Intranet potrebbero presentare verso l'esterno lo stesso indirizzo IP.
Il problema di gestione dello stato della sessione si complica ulteriormente se si vogliono rendere trasparenti i guasti agli utenti e garantire la continuità di sessione. Con tali esigenze, le sessioni eseguite da un server guasto devono essere recuperate dagli altri server che lo sostituiranno e subentreranno nell'esecuzione delle richieste seguenti degli utenti connessi al server guasto. La soluzione adottata in questi casi consiste nel memorizzare in modo permanente lo stato della sessione nel DBMS, con lo svantaggio di aumentare il carico nel sistema per l'aggiornamento dello stato della sessione. Tale soluzione deve pertanto essere introdotta se a livello applicativo è effettivamente necessario mascherare all'utente il guasto e garantire la continuità di sessione.

Il problema del mantenimento della sessione si presenta anche se vengono introdotti i protocolli HTTPS o SSL per effettuare connessioni sicure verso gli utenti. I protocolli di sicurezza infatti richiedono l'esecuzione di un protocollo piuttosto complesso che coinvolge client e server per la

generazione di una chiave di sessione che viene utilizzata poi per effettuare comunicazioni sicure attraverso schemi di crittografia simmetrica. La chiave di sessione viene generata da un server e non viene condivisa con altri server; pertanto tutte le richieste provenienti dallo stesso client devono essere indirizzate verso lo stesso server.
La figura seguente mostra come semplificare il problema introducendo un Web server dedicato alla gestione delle connessioni sicure:



Attualmente l'architettura che viene adottata nei centri di elaborazione dati prevede cinque tier con server farm. L'architettura assegna 5 tier dedicati all'esecuzione di Web Server, Script engine e Application server. Questa soluzione architetturale presenta il più alto livello di prestazioni, disponibilità e scalabilità, ma è una soluzione costosa e generalmente complessa da mantenere.



Vediamo infine un riassunto delle principali architetture e dei relativi vantaggi e svantaggi.

Configurazione architetturale	Vantaggi	Svantaggi
2 tier single host	Costo: basso, se non serve hw ad alte prestazioni Complessità: soluzione semplice da installare e manutenere Mantenimento dello stato: semplice memorizzato su una singola macchina	Prestazioni: legate alle caratteristiche della macchina, Database e Web Server competono per le risorse Scalabilità: limitata dalla possibilità di upgrade della macchina Disponibilità: se cade un componente, il sistema non è più accessibile Sicurezza: dati non difesi se il firewall viene superato
3 tier dual host	Prestazioni: dimensionamento più efficace di Web Server e DBMS server Scalabilità: possibilità di intervenire separatamente su middle tier e data tier che hanno requisiti prestazionali differenti Sicurezza: dati su macchine distinti sono più sicuri	Scalabilità: limitata dalla possibilità di upgrade della macchina Disponibilità: un componente fermo blocca ancora il sistema
3 tier e server farm	Prestazioni: distribuzione del carico di lavoro sui server/processi in modo bilanciato Scalabilità: se necessario, è possibile aggiungere nuove macchine server Disponibilità: fail-over, se cade uno dei processi, il suo carico di lavoro viene distribuito sui processi funzionanti e il sistema continua a fornire il servizio	Soluzione architetturale complessa sia in termini di gestione e configurazione sia per le problematiche di implementazione del load balancing (per il mantenimento delle sessioni) che di gestione dello stato della sessione (la memorizzazione nel DBMS è onerosa dal punto di vista delle prestazioni)
5 tier e server farm	Sicurezza: maggiore livello di sicurezza dovuto al terzo livello di firewall Prestazioni: load-balancing dinamico Scalabilità: se necessario, è possibile aggiungere nuove macchine server Disponibilità: capacità di fail-over a livello dei singoli oggetti	Complessità: ambienti generalmente complessi da manutenere

Verifichiamo le conoscenze

1. Associazione

1 Collega le caratteristiche poste a sinistra con la tipologia di architettura posta a destra:

a. 2 tier single host
b. 3 tier dual host
c. 3 tier e server farm
d. 5 tier e server farm

1. load balancing dinamico
2. massimo livello di sicurezza
3. basso costo
4. distribuzione del carico sui server in modo bilanciato
5. un componente fermo blocca il sistema

2. Collegamento

1 L'architettura 5 tier con server farm utilizza i 5 tier dedicati all'esecuzione di ....., Questa architettura ha un ..... ma è una soluzione ..... e ..... da mantenere.

2 I 4 elementi principali di un sistema Web sono:

- .....
- .....
- .....
- .....

3 L'Application server svolge il ruolo di ....., implementando la logica di ..... dell'applicazione.

4 Alcuni esempi di Application server sono:

- .....
- .....

5 Il DBMS si occupa di ..... dei dati aziendali.

6 La configurazione ..... utilizza una sola macchina fisica che supporta l'esecuzione di Web server, script engine e DBMS.

7 La configurazione ..... prevede che Web server e Script engine siano ospitati su una stessa macchina, mentre il DBMS su di una macchina dedicata.

8 La configurazione 3 tier con server farm migliora le caratteristiche di ....., ... e .....

9 Nella configurazione ..... vengono duplicati Web server e/o Script engine.

3. Vero o falso

1 Nella configurazione 5 tier con server farm è possibile aggiungere nuove macchine server. V F

2 Nella configurazione 3 tier dual host abbiamo prestazioni date da load-balancing dinamico. V F

3 Attualmente l'architettura più usata nei grandi CED (centri elaborazione dati) è quella con 5 tier con server farm. V F

4 Quando è necessario generare una pagina dinamica, il Web server interagisce con l'Application server. V F

5 L'Application server svolge il ruolo di middle tier. V F

6 Nella configurazione 3 tier dual host si vengono a creare numerosi overhead dovuti alla continua attivazione/disattivazione dei processi e apertura/chiusura delle connessioni al DBMS. V F

7 La configurazione 3 tier e dual host utilizza una DMZ. V F

8 La configurazione 2 tier e single host utilizza una DMZ. V F

LEZIONE 3

Amministrazione di una rete

In questa lezione impareremo...

- a conoscere gli elementi che concorrono all'amministrazione di una rete
- a conoscere i metodi di autenticazione
- a conoscere i servizi di directory
- a comprendere le relazioni di fiducia tra i domini

Installazione dei componenti software di un client di rete

I computer client di una rete sono generalmente rappresentati da host di tipo workstation su cui vengono eseguite applicazioni che spesso richiedono una connessione tramite la rete ai server presenti. Non richiedono particolari caratteristiche hardware o software, ma necessitano di una configurazione corretta per poter interrogare il server.
La scelta del sistema operativo è legata al programma client che si intende eseguire, alcuni software richiedono uno specifico sistema operativo mentre altri (la maggior parte) sono multipiattaforma e possono essere utilizzati su sistemi operativi diversi. L'installazione dei programmi avviene nella maniera consueta.
Per le distribuzioni Linux:

- scaricare e installare il pacchetto relativo alla distribuzione adottata;
- impostare la configurazione mediante script forniti con i sorgenti del programma oppure modificando i file di configurazione.

Per i sistemi Windows:

- eseguire il setup di installazione;
- la configurazione generalmente viene richiesta automaticamente a installazione avvenuta.

Configurazione dei protocolli di rete di un client

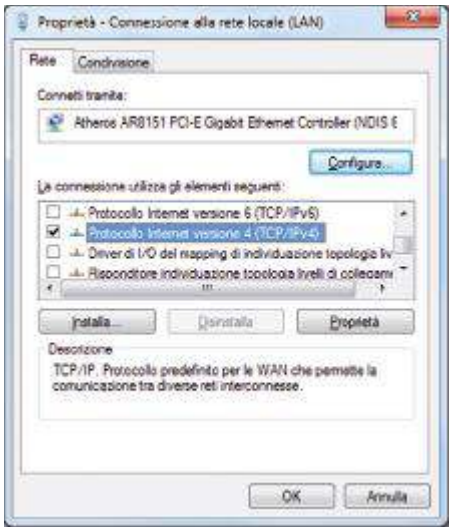
Affinché i servizi sul client funzionino correttamente è importante impostare correttamente i protocolli di rete incaricati del trasporto dei dati tra client e server. Come sappiamo il protocollo più diffuso è il TCP/IP, ma esistono tuttavia client specifici che richiedono altri protocolli, come ad esempio NetBEUI, IPX o ancora protocolli creati specificatamente per le applicazioni. Il protocollo di rete è un elemento che interagisce fortemente con il kernel del sistema operativo. Adesso ne illustreremo l'installazione in due ambienti operativi.

ESEMPIO

Installazione e configurazione del protocollo di rete TCP/IP: Windows

Installazione e configurazione del protocollo di rete TCP/IP: Windows

Selezioniamo le impostazioni della rete nel Pannello di controllo, quindi le connessioni remote e successivamente le proprietà della Connessione alla rete locale LAN.



Nella finestra che appare dobbiamo accertarci che sia presente il Protocollo Internet TCP/IP, e in caso contrario installarlo selezionando il tasto Installa e scegliendo il protocollo dalla lista dei protocolli.

Amministrazione della rete

Attraverso l' ◀ amministrazione di rete ▶ si implementano le procedure e le politiche necessarie per garantire il corretto funzionamento della rete, a partire dall'autenticazione degli utenti fino al monitoraggio e al mantenimento delle corrette funzionalità degli apparati.

◀ Con il termine amministrazione di rete si intendono l'insieme delle funzioni di gestione necessarie per garantire la corretta utilizzazione dei servizi, le funzionalità e la qualità di una rete. ▶

Vediamo come realizzare l'amministrazione di una rete, partendo proprio dall'autenticazione degli utenti e dalla regolamentazione nell'uso dei servizi, per giungere alle più tipiche funzioni di gestione e monitoraggio di rete.

L'autenticazione del client

In un sistema distribuito l'autenticazione riguarda la verifica dell'identità di un utente. Questa operazione è chiamata autenticazione del client. Sulla base di questa verifica il sistema permette o nega l'utilizzazione di risorse e/o l'esecuzione di procedure. Gli schemi adottati per l'autenticazione sono fondamentalmente 3:

- User to host. È il metodo usato dall'host per autenticare gli utenti.
- Host to host. È il metodo usato dall'host per convalidare l'identità di altri host, in modo da poter scoprire eventuali comunicazioni fraudolente.
- User to user. È il metodo usato per verificare che i dati elettronici provengano effettivamente dall'utente in questione e non da qualcuno che si spaccia per il mittente.

Le tecniche mediante le quali è possibile identificare host o user sono principalmente tre:
- Something You Are (SYA);
- Something You Know (SYK);
- Something You Have (SYH).

Possiamo riassumere le caratteristiche di queste tre tecniche nel modo seguente.

SYA

L'utente viene identificato attraverso ciò che rappresenta (something you are). A questa categoria appartengono i meccanismi di identificazione biometrica attraverso i quali l'utente viene identificato sulla base di dati fisici precedentemente impostati adattati all'utente. Le principali problematici legate a questa tipologia di autenticazione sono:
- alta percentuale di errore, stimabile nel 10%;
- rischio di intrusione nei sistemi di rilevazione;
- costo elevato delle attrezzature.

SYK

L'utente viene identificato per mezzo di quello che conosce (something you know). Questo metodo di riconoscimento funziona per mezzo di una password segreta. È sicuro quando è abbinato a tecniche crittografiche e quando le password che viaggiano sulla rete vengono cambiate spesso. Si tratta di un metodo assai efficiente ed economico.

SYH

L'utente viene identificato per mezzo di qualcosa che possiede, chiamato token che può essere presente in una smart card o in un tesserino bancomat. Per potere essere autenticato e quindi accedere al sistema l'utente deve possedere il token e, di norma, essere a conoscenza di un segreto, ad esempio un PIN o una password. Questo tipo di metodologia di identificazione può presentare i seguenti problemi:
- il token può essere smarrito, clonato o al momento non disponibile;
- il token comporta un costo che in alcuni casi può anche essere elevato;
- il corretto uso del token presuppone l'esistenza di una infrastruttura hardware e software che può essere piuttosto complessa.

A seconda di come gli schemi precedenti vengono applicati, la tecnica di autenticazione può essere:
- a fattore unico;
- a due o più fattori.

L'autenticazione a fattore unico è basata sul possesso o la conoscenza di una singola entità, ossia un elemento che solo l'utente ha a disposizione come ad esempio i dati di autenticazione (user name e password), in cui il primo fattore viene distribuito all'intera organizzazione, mentre la password è nota solo all'utente. Tali schemi non presentano un elevato grado di sicurezza: una password facile da ricordare è anche facile da indovinare. È necessario quindi definire scelte rigide per la scelta delle password, evitando facili schemi, quali date di nascita, iniziali di nomi ecc.

Gli schemi a due fattori si basano sulla memorizzazione di un'entità e sul possesso di un'altra, come ad esempio il possesso di una smart card e la conoscenza di un codice PIN. La sicurezza è migliore rispetto agli schemi a fattore unico, tuttavia risulta di scarsa praticità d'uso in quanto lega l'utente al possesso di un oggetto che deve essere a portata di mano nel momento dell'autenticazione.

> La forma di autenticazione più usata in Internet, sia per ragioni di semplicità che di economia, è la SYK a fattore unico.

Amministrazione del sistema operativo

Attualmente i sistemi operativi di rete sono altresì sistemi operativi multiutente. Più utenti possono pertanto accedere contemporaneamente al sistema utilizzando le risorse messe a disposizione dal file system. L'accesso può avvenire direttamente dalla console del computer o in generale del supporto, oppure tramite rete. La sicurezza di questi sistemi è basata sui permessi che vengono associati alle varie risorse, in modo da restringerne l'accesso ai soli utenti abilitati. Vedremo di seguito le modalità di gestione degli utenti e l'associazione delle relative autorizzazioni all'uso delle varie risorse del sistema. L'amministrazione centralizzata di un sistema viene garantita, nei sistemi Windows mediante il servizio Active Directory, che permette la creazione e la modifica di utenti, gruppi, politiche di sicurezza e autorizzazioni relative alle risorse (file, directory, stampanti).

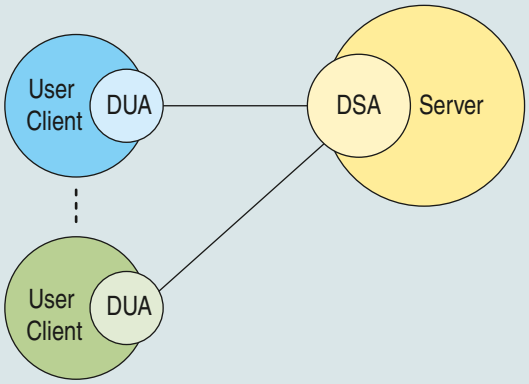
■ Servizi di directory

Un servizio di directory è una sorta di base dati distribuita di informazioni o di puntatori alle informazioni disponibili (utenti, gruppi, risorse). Consente di organizzare e gestire le informazioni riguardanti reti di computer e risorse condivise disponibili tramite la rete. L'amministratore di sistema utilizza il servizio di directory per gestire il controllo degli accessi in relazione all'utilizzo delle risorse del sistema. Possiamo affermare che i servizi di directory formano uno strato intermedio tra gli utenti e le risorse.

Una volta implementata la directory service possiamo creare applicazioni distribuite che la utilizzeranno.

Un tipico esempio di servizio di directory è rappresentato dall'elenco telefonico per la rete telefonica in cui la base dati contiene i dati delle persone e le loro proprietà associate, che sono i numeri telefonici e l'indirizzo. Una semplice applicazione potrebbe ricavare il numero telefonico dato il nome dell'utente. Il protocollo ◀ X.500 ▶ sviluppato dalla ISO è lo standard internazionale per i servizi di directory.

◀ X.500 è un'applicazione distribuita che consente l'accesso e la gestione di una base di dati logicamente strutturata ad albero chiamata Directory Information Base (DIB). Il DIB è gestito e reso disponibile da un numero, ipoteticamente infinito, di Directory Service Agents (DSA). Gli utenti del servizio sono rappresentati da Directory User Agents (DUA). Gli utenti del servizio sono processi applicativi che usano X.500 per migliorare il servizio che offrono agli utenti finali. ▶



Il protocollo X.500 specifica lo schema di default con cui costruire la base dati e descrive alcune Directory Information Tree (DIT).
Le directory basate sul protocollo X.500 permettono di creare oggetti che contengono altri oggetti e supportano relazioni gerarchiche. L'albero delle informazioni viene costruito in base ai valori di attributi delle informazioni che possono essere di tipo assolutamente generale. In una directory X.500 deve essere possibile reperire gli oggetti secondo schemi di ricerca, per esempio basati sui nomi degli attributi di un oggetto. Ogni elemento del DIB può essere ritrovato utilizzando due diverse notazioni.

- Distinguished Name (DN) che identifica univocamente l'elemento nell'albero.
- Relative Distinguished Name (RDN) che identifica univocamente l'oggetto all'interno di uno specifico contesto, ossia come elemento all'interno di una parte dell'albero.

Esiste una versione semplificata chiamata LDAP (Lightweight DAP) che viene utilizzata per accedere a servizi di directory in Linux e Windows.

ESEMPIO

Directory del personale della scuola

In questo esempio vogliamo organizzare un albero di directory di una scuola, in cui la directory del personale della scuola viene organizzato tramite attributi che identificano le mansioni del personale stesso. Partendo dalla radice del DIT possiamo inserire come attributo la Sezione di appartenenza (S) e un secondo legato all'attività specifica nell'ambito della sezione (A) e infine un terzo che identifica la persona per Nome e Cognome (CN).

Root
S=Amministrazione
S=Docenti
A=Informatica
CN=Verdi Luca
CN=Marelli Adriano
A=Matematica
CN=Rossi Tiziana
CN=Russo Adele
...
S=Tecnici
A=lab.fisica
CN=Bonatti Andrea
...

Come possiamo vedere all'interno di questa struttura Bonatti Andrea è identificato utilizzando il distinguished name:

```
DN={S=Tecnici,A=lab.fisica,CN=Bonatti Andrea}
```

oppure all'interno della parte di albero relativo ai tecnici del laboratorio di fisica dal relative distinguished name:

```
RDN={CN=Bonatti Andrea }
```

Un sistema distribuito può avvalersi di uno o più directory service per la catalogazione dei nomi e degli attributi degli elementi del sistema (utenti, gruppi o computer).

LDAP

Lightweight Directory Access Protocol (LDAP) è un sistema di gestione centralizzata di informazioni, che viene usato anche nella gestione di dati generici quali bookmarks o indirizzari. L'aggettivo lightweight (leggero) indica che la progettazione del sistema privilegia le prestazioni, essendo infatti studiato per ottenere risposte in tempi rapidi nella ricerca e lettura dei dati, a scapito di una maggiore lentezza nelle operazioni di scrittura e aggiornamento. Questo non rappresenta un problema grave, in quanto le operazioni di scrittura avvengono di norma meno frequentemente rispetto a quelle di lettura, basti pensare ad esempio a quante volte consultiamo la nostra rubrica telefonica rispetto a quante volte invece la modifichiamo.
LDAP gestisce i dati secondo una organizzazione gerarchica ad albero di directory in cui i singoli elementi possono avere più attributi. Gli elementi di una directory, nodi intermedi o foglie dell'albero, possono anche essere riferimenti ad altre directory residenti su altri server LDAP. Ogni elemento deve avere un nome che permetta di individuarlo in modo univoco nella directory. Alcuni dei tipi possibili utilizzabili per definire gli attributi di un oggetto sono i seguenti:

- bin: dato binario;
- ces (case exact string): stringa in cui vengono distinte le lettere maiuscole dalle minuscole;

- cis (case ignore string): stringa in cui le lettere maiuscole e minuscole sono trattate allo stesso modo
- tel: numero telefonico;
- dn (distinguished name): nome univoco.

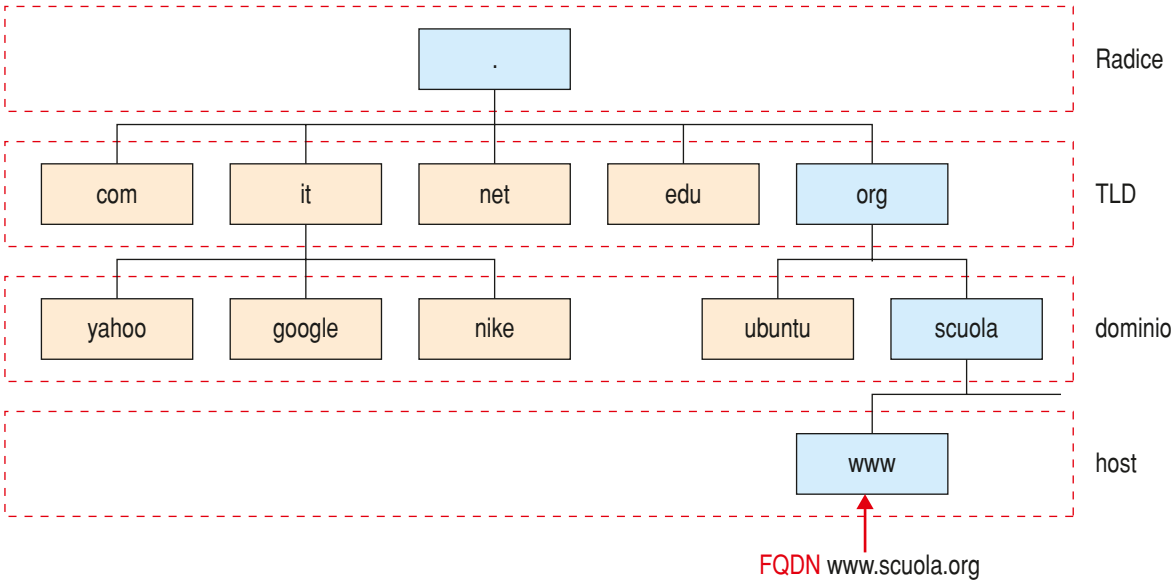
Un server che fornisce il servizio LDAP in Linux è slapd. Il servizio di directory LDAP è basato su un modello client-server in cui uno o più server LDAP contengono i dati che costituiscono l'albero di directory di LDAP o il database LDAP sottostante. Un client LDAP si collega a un server LDAP ed effettua una richiesta, quindi il server risponde oppure indica al client dove poter ottenere maggiori informazioni mediante ad esempio un altro server LDAP. Non importa a quale server LDAP un client si connetta poiché esso avrà sempre la stessa vista dell'albero di directory.

DNS

Il Domain Name System (DNS) è uno dei più noti e utilizzati servizi di directory, fondamentale nel meccanismo di funzionamento della rete Internet. Alle origini del TCP/IP, dato che le reti erano poco estese o detto in un altro modo il numero di computer connessi a una stessa rete era basso, gli amministratori di rete crearono dei fili detti tabelle di conversione manuale che associavano a ogni linea l'indirizzo IP del terminale e il nome letterale associato, detto nome dell'host. Questo metodo necessitava tuttavia dell'aggiornamento manuale delle tabelle di tutti i computer in caso di aggiunta o modifica di un nome di terminale, venne quindi realizzato il sistema di gestione dei nomi gerarchizzato, chiamato appunto Domain Name System (DNS) nel 1983. Questo sistema propone:

- uno spazio di nomi gerarchico che permette di garantire l'unicità di un nome in una struttura ad arborescenza, basato sullo stile del file system di Unix;
- un sistema di server distribuiti che permette di rendere disponibile lo spazio dei nomi;
- un sistema di client che permette di risolvere i nomi dei domini, interrogando i server per ottenere l'indirizzo IP corrispondente a un nome.

Come sappiamo la struttura del sistema DNS è ad albero dove i domini di livello superiore, chiamati TLD (Top Level Domains), sono collegati a un nodo radice rappresentato da un punto, come indicato nella seguente figura:



Ciascun nodo dell'albero viene chiamato nome del dominio, e può avere un nome lungo al massino 63 caratteri. L'insieme dei nomi di dominio costituisce quindi un albero inverso dove ogni nodo è separato dal seguente da un punto (.) secondo la dot notation. Il nodo foglia della struttura ad albero è rappresentato dall'host, in questo caso chiamato www, inoltre il nome di tale host deve essere unico nel dominio considerato. Nel dettaglio dobbiamo però affermare che il termine dominio corrisponde formalmente al suffisso di un nome di dominio, cioè l'insieme delle etichette dei nodi a eccezione dell'host.
Il nome completo di un dominio è chiamato FQDN (Fully Qualified Domain Name) e ha una profondità massima di 127 livelli, con un nome lungo al massimo 255 caratteri. L'indirizzo FQDN permette di individuare inequivocabilmente un terminale sulla rete di reti.

I server di nomi

I computer chiamati server di dominio permettono di stabilire la corrispondenza tra il nome del dominio e l'indirizzo IP dei terminali di una rete. Ogni dominio possiede un server di nomi di domini, chiamato PDNS (Primary Domain Name Server), cioè server di nomi primario oltre a un altro server chiamato server di nomi secondario (SSDNS – Secondary Domaine Name Server), che permette di sostituirsi al server di nomi primario in caso di indisponibilità. Ciascun server di nomi è dichiarato in un server di nomi di dominio di livello immediatamente superiore, cosa che permette implicitamente una delega di autorità sui domini.
Il sistema di nomi è anch'essa un'architettura distribuita, dove ogni entità è responsabile della gestione del proprio nome di dominio. Non esiste quindi un organismo che abbia il compito di gestire l'insieme dei nomi di domini. I server corrispondenti ai domini di più alto livello (TLD) sono chiamati server di nomi radice. Ne esistono tredici, ripartiti in tutto il mondo, sotto i nomi che vanno dalla lettera "a" fino alla "m":

a.root-servers.net
...
m.root-servers.net

Un server di nomi definisce una zona, cioè un insieme di domini sui quali il server ha autorità. Il sistema di nomi di dominio è trasparente per l'utente, tuttavia non bisogna dimenticare i punti seguenti.

- Ogni computer deve essere configurato con l'indirizzo di un terminale capace di trasformare qualunque nome in un indirizzo IP. Questo terminale è detto Domain Name Server. Niente panico: quando vi connettete a Internet, il fornitore dell'accesso modifica automaticamente i vostri parametri di rete per mettervi a disposizione questi server di nomi.
- L'indirizzo IP di un secondo Domain Name Server (secondary Domain Name Server) deve essere ugualmente definito: il server di nomi secondario può sostituire il server di nomi primario in caso di malfunzionamento del primo.

Directory services in Windows

Il sistema operativo Windows in versione server è pienamente compatibile con lo standard X.500 per quanto riguarda il servizio di directory. Il servizio di directory di Windows Server è chiamato Active Directory, e mette a disposizione al NOS (Network Operating System) una directory di oggetti specifici che consente di gestire gli utenti con le relative proprietà, oltre ad altre funzionalità specifiche come i volumi DFS (Distributed File System), gli oggetti GPO (Group Policy Object) e l'infrastruttura PKI (Public Key Infrastructure).

Il tipi di oggetti che possono essere contenuti in una directory sono potenzialmente illimitati, anche se dobbiamo tuttavia occorre tenere conto delle prestazioni che vengono limitate dall'uso eccessivo di oggetti.

I domini

In una rete basata sul sistema operativo di rete (NOS) di tipo Windows Server un ◀ dominio ▶ costituisce un contesto di sicurezza separato.
L'amministratore di un dominio possiede infatti tutti i permessi e i diritti necessari per svolgere qualsiasi attività all'interno del proprio dominio, ma non ha nessun permesso né nessun diritto in altri domini a meno che non gli vengano esplicitamente garantiti. Ogni dominio possiede quindi le proprie politiche di sicurezza come ad esempio il controllo sulla composizione delle password e sul tempo di vita degli account utente.

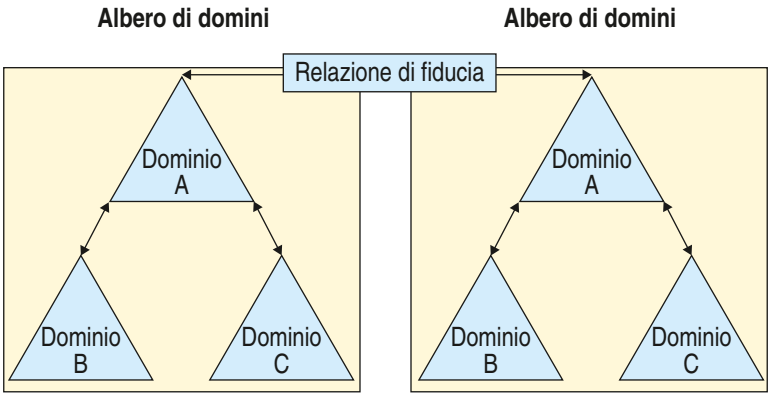
◀ Un dominio è un insieme di computer, comunicanti tra loro e che condividono un directory database comune. ▶

I domini sono anche Unità di Replica, infatti tutti i Controllori di Dominio possiedono una copia completa delle informazioni di directory del proprio dominio e replicano tra loro le modifiche. Il modello di replica è di tipo multi master dove tutti i controllori di dominio hanno accesso in lettura e scrittura alla copia delle informazioni di directory in loro possesso, replicano le modifiche a tali informazioni agli altri controllori di dominio e ricevono le modifiche apportate dagli altri.

Windows versione server, a partire dalla versione 2003, non utilizza più i nomi di dominio secondo lo standard chiamato NetBIOS che ne limitava la lunghezza a quindici caratteri. Questa decisione è strettamente legata alle problematiche legate alla sicurezza anche se questo tipo di nomi risulta ancora presente.

Albero di domini

Un albero di domini è costituito da un insieme di domini che si accordano vicendevolmente la fiducia e che appartengono a uno spazio di nomi contiguo, come ad esempio un albero di directory in cui ciascun dominio è un sotto-dominio del proprio dominio padre. Un esempio di spazio di nomi contiguo è rappresentato da un albero di domini che contiene alla radice il dominio scuola.local, un dominio figlio chiamato sistemi.scuola.local sotto quest'ultimo, e un ulteriore dominio figlio chiamato lab1.sistemi.scuola.local. In tal modo otteniamo tre domini che formano un albero di domini rappresentato da uno spazio di nomi contiguo.



Foresta di domini

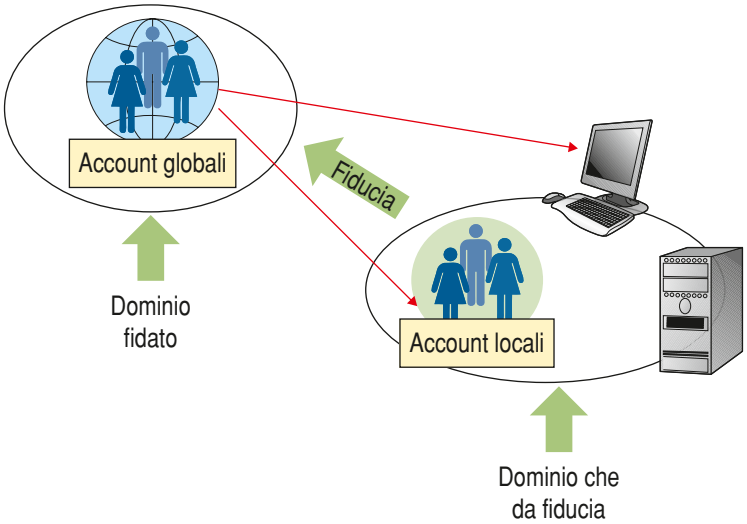
Una foresta di domini è costituita da un albero di domini o da un insieme di alberi di domini, caratterizzato da spazi di nomi contigui separati. Quando nell'ambiente viene installato il primo controller sul primo dominio del primo albero, è necessario specificare se appartiene a una nuova foresta oppure a una foresta già esistente. In Active Directory, tutti i domini di una foresta devono condividere il me-

desimo schema. In genere i NOS non consentono di fondere più foreste o schemi, quindi per creare più foreste, come ad esempio quando la società si fonde con un'altra che dispone già di una foresta Active Directory, occorre utilizzare relazioni di fiducia che vengono illustrate nel prossimo paragrafo.

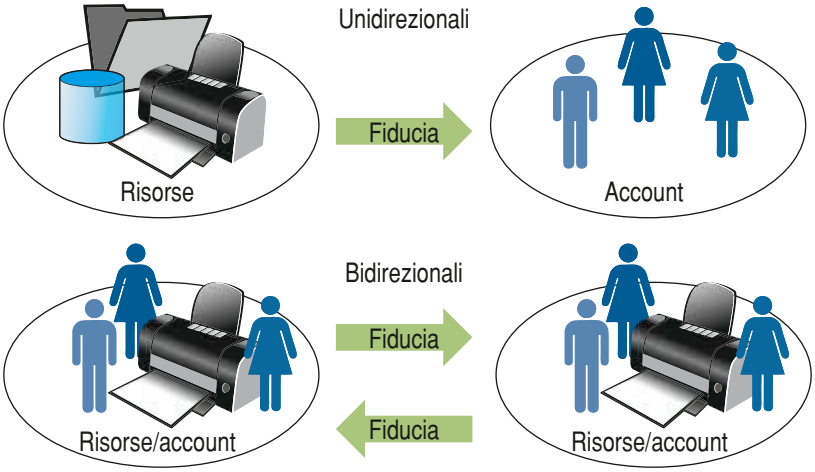
Le relazioni di fiducia

Le relazioni di fiducia (◀ Trusted relationships ▶) consentono l'accesso alle risorse dell'intera rete con un unico account di dominio e subendo un unico processo di logon.

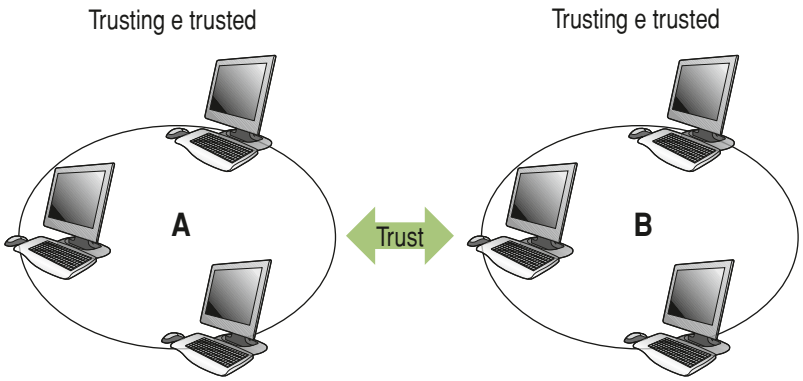
◀ La relazione di fiducia è generalmente espressa in termini di una relazione binaria tra un soggetto (trustor) che si fida di un altro soggetto, il fiduciario (trustee).
Può anche essere una relazione:
- uno-a-molti, che si può applicare a un gruppo di entità come fiduciario;
- molti-a-molti, come la fiducia reciproca tra i membri di un gruppo;
- molti-a-uno, tra diversi soggetti verso un unico soggetto. ▶



Spesso non è simmetrico: la fiducia di A in B di solito non è la stessa fiducia di B in A o è a senso unico. La fiducia è soggettiva: dato lo stesso fiduciario, avrò diversi livelli di fiducia da parte di soggetti diversi. La figura seguente mostra una fiducia unidirezionale e bidirezionale:



Inoltre permettono la fusione di amministrazione locale e centralizzata secondo un percorso monodirezionale o bidirezionale. In questo caso A concede l'accesso delle sue risorse a B e B concede ad A l'accesso alle sue risorse.



Gli account utente locali non possono essere esportati in altri domini per utilizzarne risorse. Sono concessi agli utenti di domini untrusted o provenienti da altri ambienti di sistema.

Gli account utente globali possono invece essere esportati per l'utilizzo di risorse di altri domini.

I gruppi locali raggruppano gli utenti con le stesse esigenze di accesso alle risorse in locale e possono contenere:
- account utenti del dominio in cui sono stati creati;
- account utenti globali provenienti da domini trusted;
- account di gruppo globali provenienti da domini trusted;

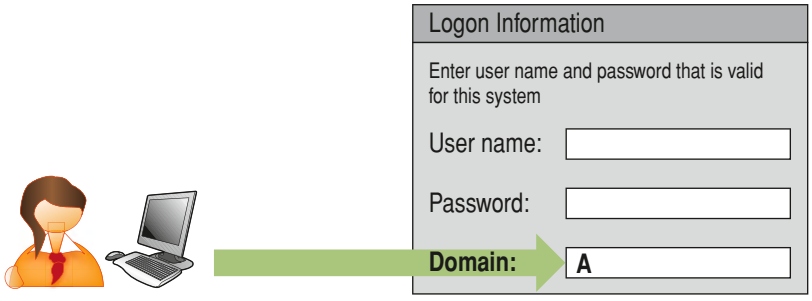
a essi possono essere assegnati diritti nel dominio in cui sono stati creati.

I gruppi globali raggruppano gli utenti con le stesse esigenze di accesso alle risorse in remoto e possono contenere soltanto account utenti globali del gruppo in cui sono stati creati. Possono essere inseriti nei gruppi locali dei domini trusting, mentre a essi possono essere assegnati diritti nel dominio in cui creati o nei domini trusting in cui esportati.

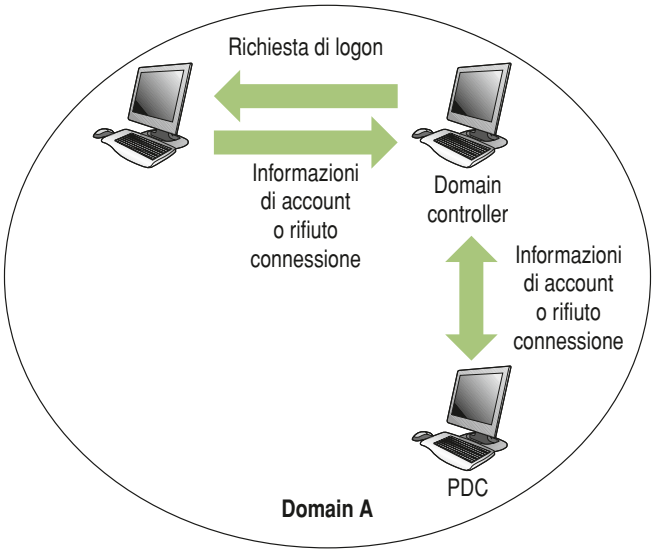
Vediamo come viene gestito il processo di ◀ logon ▶ attraverso diverse relazioni di fiducia.

◀ Il processo di logon è la prima misura di sicurezza per proteggere le risorse da accessi illeciti. Consiste di una fase di inserimento informazioni (user name e password, dominio) e una fase di autenticazione. ▶

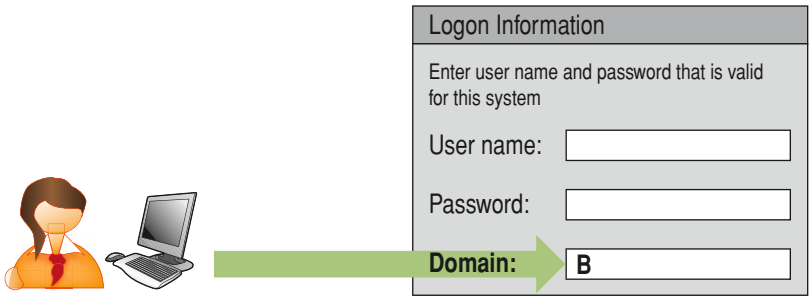
Primo caso, nella procedura di logon in locale l'utente possiede un account nel dominio A e si collega a una macchina sempre all'interno del dominio A:



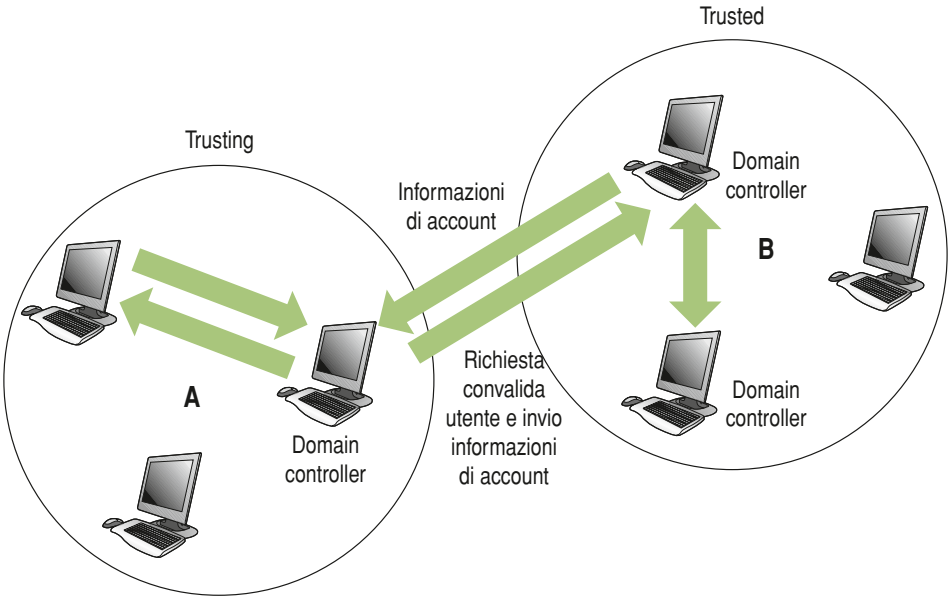
Nel dettaglio avviene un processo di autenticazione pass-through come indicato dall'immagine seguente:



Vediamo un secondo caso, l'utente possiede un account nel dominio B e si collega a una macchina del dominio A. Il logon procede come se l'utente si stesse collegando con un account locale alla macchina:



Nel dettaglio avviene un processo di autenticazione pass-through come indicato dall'immagine seguente:



Verifichiamo le conoscenze

1. Completamento

1 Affinché i servizi sul client funzionino correttamente è importante impostare correttamente i ..... incaricati del trasporto dei dati tra ..... e .....

2 Attraverso l' ..... si implementano le procedure e le politiche necessarie per garantire il corretto funzionamento della rete.

3 In un sistema distribuito l' ..... riguarda la verifica dell'identità di un utente.

4 ..... è il metodo usato per verificare che i dati elettronici provengano effettivamente dall'utente in questione e non da qualcuno che si spaccia per il mittente.

5 ..... è il metodo usato dall'host per autenticare gli utenti.

6 ..... è il metodo usato dall'host per convalidare l'identità di altri host.

7 Le tre tecniche mediante le quali è possibile identificare host o user sono:

- ..... la cui sigla è (.....)
- ..... la cui sigla è (.....)
- ..... la cui sigla è (.....)

8 Nell'autenticazione a fattore unico è necessaria la conoscenza di ..... che solo l'utente ha a disposizione come ad esempio .....

9 Gli schemi a due fattori si basano sulla memorizzazione di un'entità e sul possesso di un'altra, come ad esempio ..... e la conoscenza di .....

10 L'amministrazione centralizzata di un sistema, nel NOS Windows, è garantita da ....., che permette la creazione e la modifica di ..... e .....

11 Il protocollo ..... sviluppato dalla ISO è lo standard internazionale per i servizi di directory.

12 ..... è un sistema di gestione centralizzata di informazioni, che viene usato anche nella gestione di dati generici quali bookmarks o indirizzari.

13 DNS utilizza ..... che permette di garantire l'unicità di un nome in una struttura ad albero, un ..... che permette di rendere disponibile lo spazio dei nomi e un ..... che permette di risolvere i nomi dei domini, interrogando i server per ottenere l'indirizzo IP corrispondente a un nome.

14 I domini sono anche delle ....., in quanto tutti i controllori di dominio possiedono una copia completa delle informazioni di directory del proprio dominio e replicano tra loro le modifiche.

2. Vero o falso

1 La configurazione dei software client nei sistemi Windows è richiesta automaticamente a installazione avvenuta. V F

2 Il protocollo di rete è un elemento che interagisce fortemente con il kernel del sistema operativo. V F

3 Il metodo usato dall'host per autenticare gli utenti prende il nome di Host to host. V F

4 Mediante la tecnica SYA l'utente viene identificato sulla base di dati biometrici precedentemente impostati adattati all'utente. V F

5 Mediante la tecnica SYH l'utente viene identificato per mezzo di quello che conosce, come ad esempio una password segreta. V F

6 Un servizio di directory è una sorta di base dati distribuita di informazioni o di puntatori alle informazioni disponibili. V F

7 LDAP gestisce i dati secondo una organizzazione gerarchica ad albero di directory in cui i singoli elementi possono avere più attributi. V F

8 I computer chiamati server di dominio permettono di stabilire la corrispondenza tra il nome del dominio e l'indirizzo IP dei terminali di una rete. V F

LEZIONE 4

Active Directory

In questa lezione impareremo...

- a conoscere gli oggetti principali gestiti Active Directory
- a capire il ruolo di Active Directory nella gestione di un NOS
- a definire le policies del sistema
- a gestire i criteri di gruppo, i permessi NTFS e le condivisioni

Active Directory

Active Directory è un database integrato nei sistemi operativi di rete (NOS, Network Operative System) server Windows che fungono da Domain Controller e consente di catalogare e gestire in modo centralizzato risorse di vario genere come: utenti, gruppi di lavoro, stampanti, cartelle condivise ecc.

Active Directory è strutturata gerarchicamente ed è un contenitore di oggetti che possiamo così suddividere:

- utenti;
- gruppi;
- computer;
- domini;
- stampanti;
- unità organizzative.

Gli oggetti possono essere divisi in due categorie, oggetti veri e propri e oggetti contenitori, questi ultimi sono rappresentati da domini e unità organizzative.

I criteri di gruppo

Attraverso i criteri di gruppo (Group Policy) possiamo definire le procedure per configurare e gestire la sicurezza nel proprio ambiente. Esse costituiscono un valido aiuto per implementare raccomandazioni tecniche nei criteri di protezione di tutte le workstation e i server presenti nei propri domini Active Directory. I criteri di gruppo hanno la funzione di semplificare il controllo centralizzato o decentralizzato su privilegi, autorizzazioni e funzioni di utenti e computer di un dominio.

Con i criteri di gruppo possiamo:
- gestire in modo centralizzato cartelle speciali, come ad esempio il desktop degli utenti;
- controllare o limitare l'accesso alle risorse del computer o a quelle di rete, limitare l'accesso al pannello di controllo, alla configurazione del desktop, a quella del menu start;
- definire degli script per gli utenti, ad esempio quelli da utilizzare durante il logon;
- configurare i criteri di accesso.

I criteri di gruppo possono essere applicati a un dominio, a più domini, a unità organizzative, a singoli computer, a gruppi di utenti, a singoli utenti.

> I criteri di gruppo applicabili solo a sistemi individuali sono detti criteri di gruppo locali e sono memorizzati sul computer locale. Gli altri criteri di gruppo, riferiti a entità superiori, sono oggetti di Active Directory.

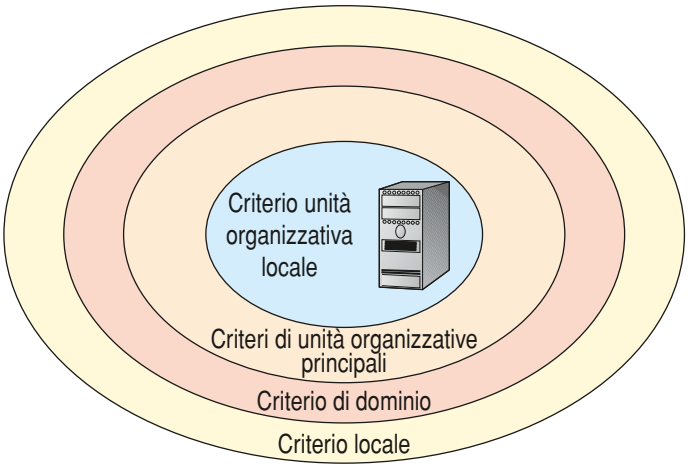
L'ordine dei criteri di gruppo

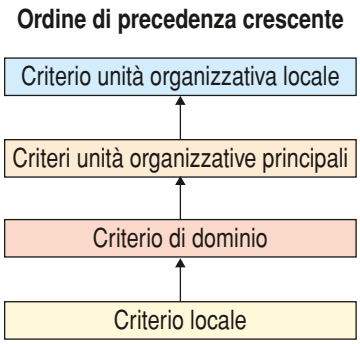
I criteri di gruppo vengono applicati secondo l'ordine seguente.
1. criteri di Windows;
2. criteri di gruppo locale;
3. criteri di sito;
4. criteri di dominio;
5. criteri di unità organizzativa;
6. criteri di unità organizzativa figlia.

Gli oggetti criteri di gruppo locali (LGPO) sono elaborati per primi, e sono seguiti da quelli di dominio. In caso di conflitto, i criteri di dominio prevalgono su quelli locali. Negli oggetti criteri di gruppo (GPO) i criteri applicati per ultimi hanno la precedenza su quelli applicati per primi, secondo l'ordine già indicato:

L S D O U

I criteri di gruppo vengono applicati secondo la seguente gerarchia:

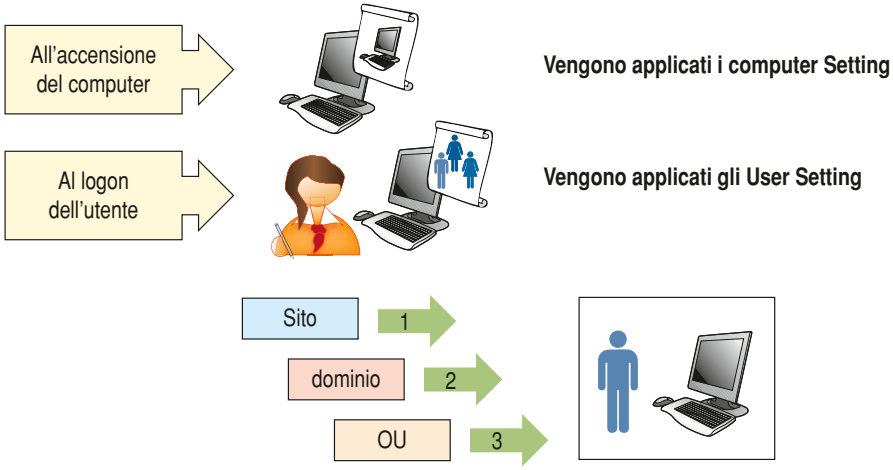




Le impostazioni dei criteri di gruppo sono classificabili in:
- impostazioni applicabili ai computer;
- impostazioni applicabili agli utenti.

Vediamo come vengono applicati i criteri riassumendo tutte le operazioni dall'avvio del server.
1. all'avvio della rete sono applicati i criteri del computer, uno per volta secondo il criterio già visto;
2. segue l'esecuzione di script di avvio, in ordine sequenziale, con inizio del successivo al termine del precedente;

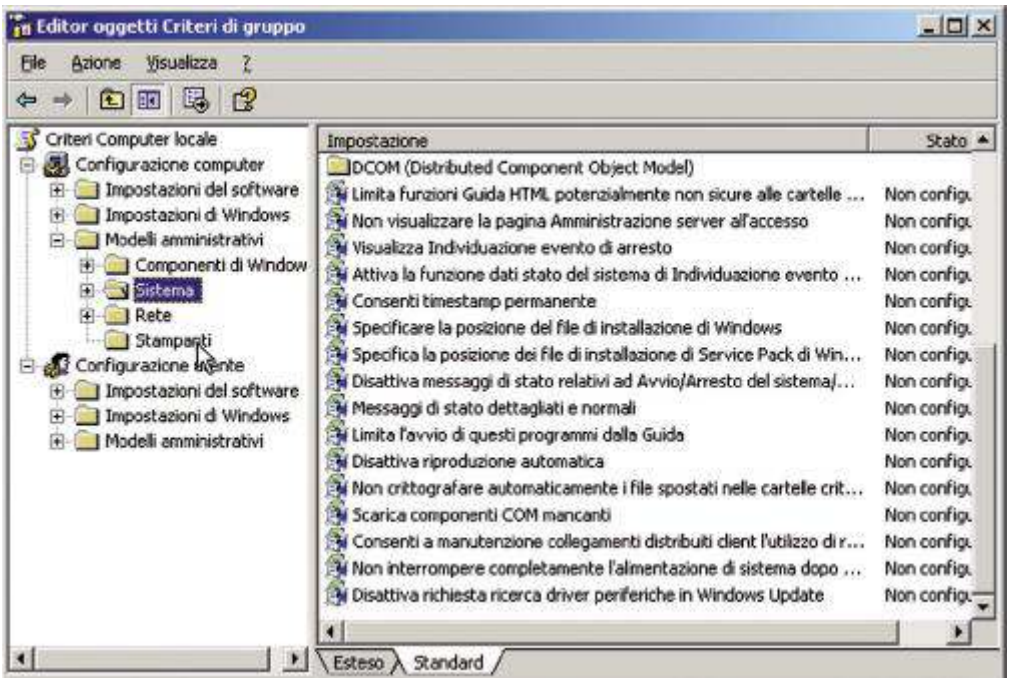
3. l'utente effettua il logon e ne viene caricato il profilo;
4. Windows Server applica i criteri utente, secondo l'ordine già visto;
5. sono eseguiti eventuali script di accesso in modo simultaneo;
6. viene infine visualizzato il desktop definito nei criteri di gruppo.



Le impostazioni di configurazione di criteri di gruppo sono memorizzate in due posizioni:
- negli oggetti criteri di gruppo contenuti in Active Directory;
- nei file modelli di protezione contenuti nel file system locale.

La console Criteri di gruppo

La console dei criteri di gruppo consente di configurare i criteri diritti utenti sia in modo locale e, quindi, riferiti solo a utenti di un computer locale, sia per gruppi esistenti in un dominio e, pertanto, applicarli agli account per tutti i computer del dominio.
Per aprire la console Criteri di gruppo dobbiamo aprire l'Editor Criteri di gruppo locali dalla riga di comando facendo clic sul pulsante Start, digitando poi gpedit.msc:



Sezione dei criteri	Significato
Criteri account Criterio password	Configurazione della validità, della lunghezza e della complessità delle password
Criteri account Criterio di blocco account	Configurazione della durata, dei limiti e dei contatori di reimpostazione dei blocchi
Criteri locali Criterio di controllo	Attivazione/disattivazione della registrazione di eventi specifici
Criteri locali Diritti utente	Definizione di diritti, quali accesso locale, accesso dalla rete e così via
Criteri locali Opzioni di protezione	Modifica di specifici valori del Registro di sistema relativi alla sicurezza
Registro eventi	Attivazione del monitoraggio delle operazioni riuscite e non riuscite
Gruppi con restrizioni	Possibilità per gli amministratori di controllare l'appartenenza a uno specifico gruppo
Servizi di sistema	Controllo della modalità di avvio di ciascun servizio
Registro di sistema	Configurazione delle autorizzazioni per le chiavi del Registro di sistema
File system	Configurazione delle autorizzazioni per cartelle, sottocartelle e file

I permessi di NTFS

NTFS è il file system di Windows dalla versione XP. I permessi ◀ NTFS ▶ possono essere utilizzati per limitare l'accesso, in locale o attraverso la rete, a determinate risorse.
Una applicazione pratica di un permesso è quello che ad esempio impedisce l'accesso a Internet a certi utenti, impedendo loro di accedere a risorse quali il browser, il programma di posta elettronica News, di FTP ecc.
Grazie al file system NTFS possiamo specificare particolari permessi di accesso per le cartelle e per i singoli file a utenti (user) o gruppi di utenti (group) in modo da proteggere le risorse del sistema e renderle fruibili solo agli utenti autorizzati. I permessi di NTFS vengono rilasciati secondo la strategia (policy) chiamata: AGDLP (Account, Global, Universal, Domain Local, Permission).

◀ NTFS è l'acronimo di New Technology File System, ed è il file system dei sistemi operativi basati su kernel NT. ▶

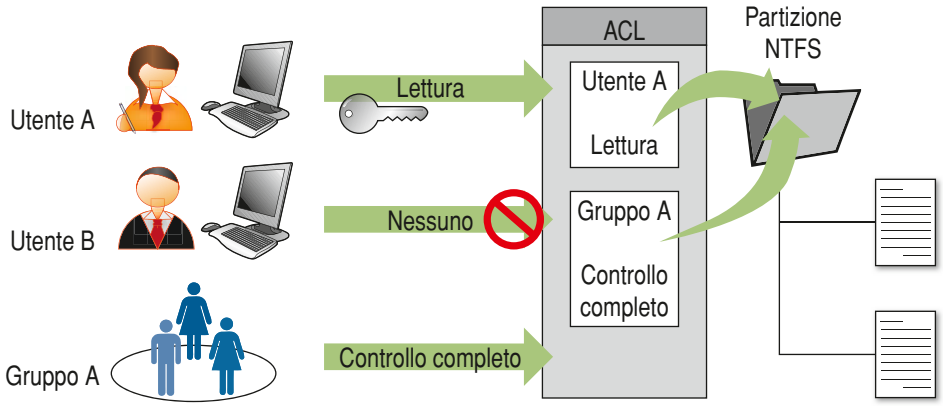
L'inibizione all'uso di risorse locali del computer può anche avvenire verso gli utenti generici per mezzo di strumenti diversi quali regedit oppure Servizi.

La strategia AGDLP prevede l'aggiunta di un Account utente a un Gruppo Globale, quindi l'inserimento di questo in un Gruppo Locale al Dominio e per finire la definizione dei Permessi a quest'ultimo. Analizziamone le fasi:

1. A per prima cosa dobbiamo definire gli user Account;
2. G quindi li dobbiamo collocare nei Gruppi globali;
3. DL poi dobbiamo inserire i gruppi globali nei Domain Local group;
4. P infine dobbiamo assegnare i permessi per l'accesso alle risorse, ai singoli gruppi locali del dominio.

NTFS consente di associare a ogni file o cartella una Access Control List (ACL) contenente gli utenti e i gruppi che possono accedere alla risorsa e i relativi permessi. L'ACL di ciascuna risorsa deve contenere almeno una Access Control Entry (ACE) associata a un utente o a un gruppo in modo da concederne l'accesso.

La figura seguente mostra come l'UtenteA e il GruppoA hanno accesso alla risorsa essendo presenti nella ACL, mentre l'UtenteB non essendo presente nella ACL non ha accesso alla risorsa.

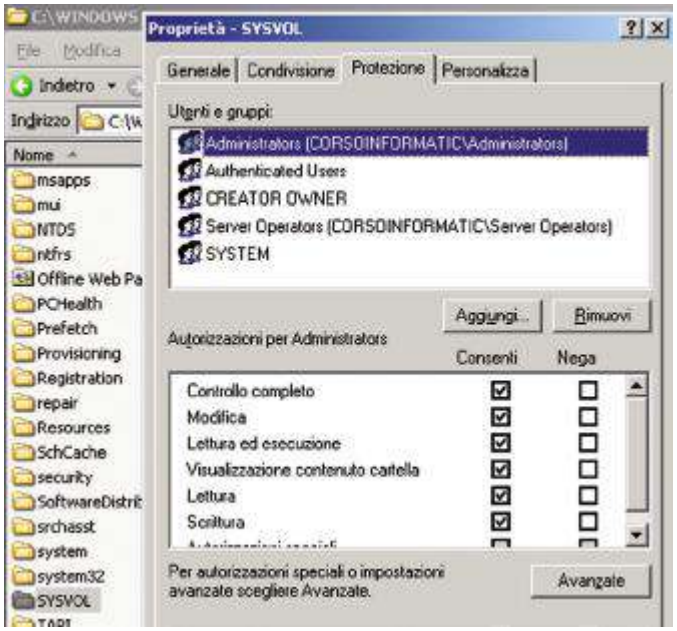


I permessi NTFS riferiti alle cartelle

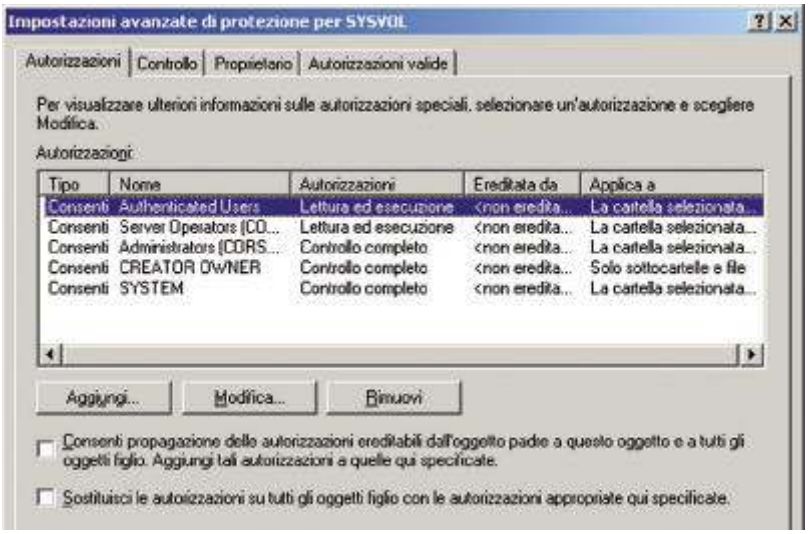
I permessi di NTFS che riguardano le directory (folder) consentono l'accesso alle cartelle, alle sottocartelle e ai file in esse contenuti. I permessi disponibili in Windows Server sono i seguenti:

- Read. Consente la visualizzazione dei file e delle sottocartelle presenti nella cartella con gli attributi, le proprietà e i permessi.
- Write. Consente di creare nuovi file e sottocartelle all'interno della directory, oltre a cambiarne gli attributi. Questo attributo permette la visione dei permessi e delle proprietà assegnate alle cartelle.
- List Folders Contents. Permette di visualizzare i nomi dei file e delle sottocartelle della directory.
- Read & Execute. Naviga attraverso le cartelle, in più permette tutte le azioni permesse dalle autorizzazioni di Read e List – Folder Contents.
- Modify. Consente la cancellazione della directory oltre ai permessi Write e Read & Execute.
- Full Control. Consente di modificare i permessi assegnati e cancellarne le sottocartelle e i file. È l'insieme di tutti i permessi precedenti.

Nella figura a fianco possiamo notare come il gruppo Administrators possieda tutte le autorizzazioni sulla cartella SYSVOL.



I permessi completi sono visibili con il pulsante Avanzate:



I permessi NTFS riferiti ai file

I permessi di NTFS permettono di gestire anche i permessi relativi ai file, infatti consentono sia l'accesso che le operazioni sui singoli file. Vediamo l'elenco dei principali permessi NTFS sui file.

- Read. Consente di visualizzare i file con i relativi attributi, le proprietà e i permessi.
- Write. Consente di creare nuovi file, cambiarne gli attributi, oltre a visualizzarne i permessi e le proprietà.
- List Folders Contents. Consente di visualizzare i nomi dei file e delle sottocartelle contenute in una cartella.
- Read & Execute. Consente di caricare le applicazioni, oltre a effettuare le azioni concesse da Read.
- Modify. Consente di modificare e cancellare i file oltre a effettuare le azione permesse da Write e Read & Execute.
- Full Control. Consente il controllo completo dei file che possiedono questo permesso, quindi può modificarne i permessi, oltre a concedere tutte le autorizzazioni NTFS viste fin qui.

Nel caso di permessi di file che contrastino con quelli delle cartelle dobbiamo ricordare che prevalgono quelli sui file rispetto a quelli della cartella che li contiene.

Nell'esempio illustrato a fianco il gruppo Administrators possiede tutte le autorizzazioni sul file SAM.LOG: ▶

I permessi specifici del file hanno sempre la precedenza sui permessi di gruppo e su quelli ereditati.

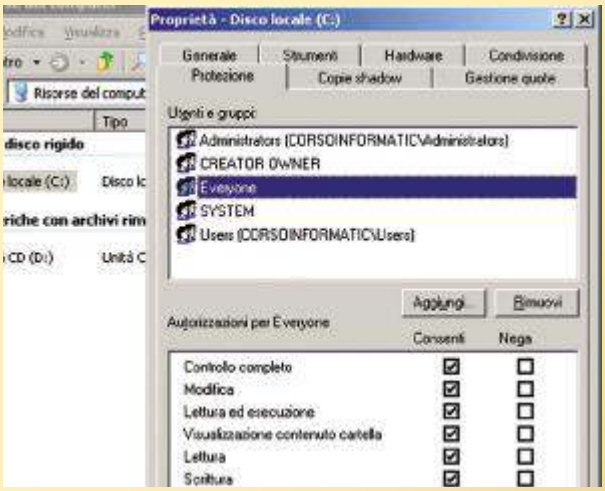
Copiando o spostando file o cartelle tra volumi NTFS, si hanno diversi risultati:

Operazione	Risultato
Copia nella stessa partizione	La copia eredita i permessi della cartella di destinazione
Copia su altra partizione, sempre NTFS	La copia eredita i permessi della cartella di destinazione
Copia su partizione non di tipo NTFS	Si perdono tutti i permessi
Spostamento sulla stessa partizione	Lo spostamento porta con sé tutti i permessi
Spostamento su altra partizione, sempre NTFS	Si ereditano i permessi della cartella di destinazione
Spostamento su partizione non di tipo NTFS	Si perdono tutti i permessi

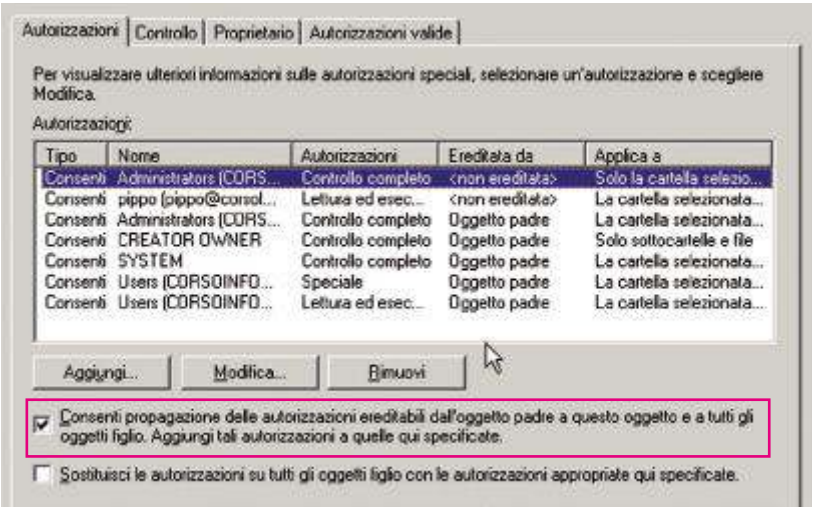
Assegnazione dei permessi NTFS

L'assegnazione di permessi NTFS a un file o a una cartella sono consentiti solo al gruppo Administrators, che possiede su quel file o su quella cartella il permesso di Full control o ne è il Proprietario.

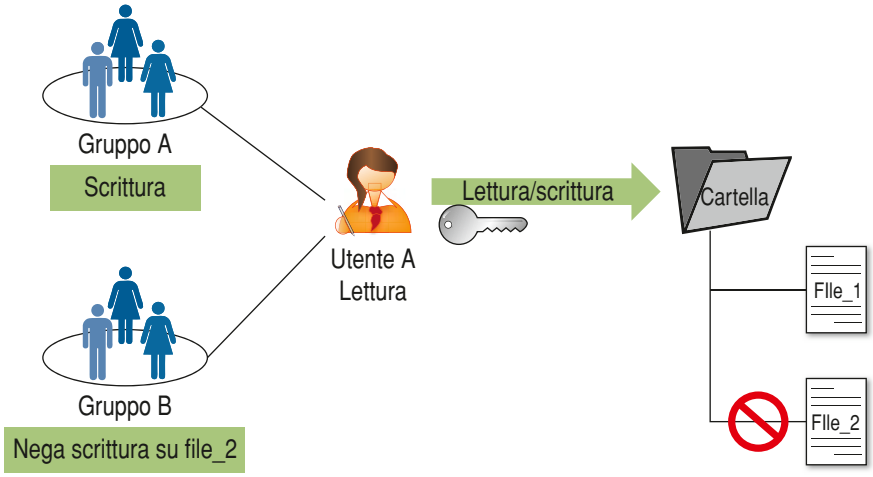
Ogni volta che installiamo una partizione NTFS è consigliabile assegnare all'unità logica il permesso Full control all'utente Everyone. In tal tutte le cartelle e i file creati in quella partizione erediteranno tale autorizzazione di default. Questo per evitare conflitti di assegnazione di permessi dato che prevale sempre il più restrittivo.



Per far propagare i permessi NTFS, assegnati a una cartella, in modo gerarchico, a tutte le cartelle e file in essa contenuti dobbiamo spuntare la casella indicata nella finestra seguente.



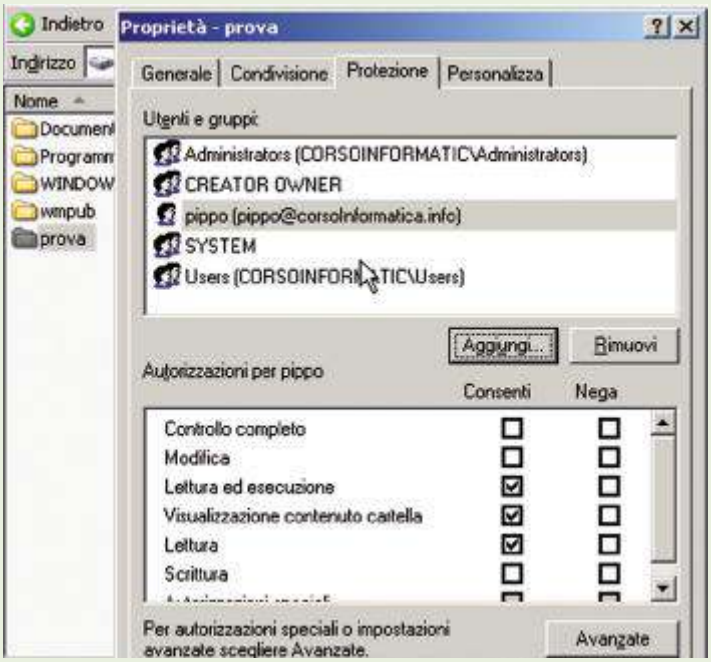
Facciamo clic sul pulsante Avanzate presente nelle proprietà della cartella. Le autorizzazioni negate prevalgono sempre su quelle concesse, inoltre i permessi NTFS sono cumulativi. Significa che se un utente possiede dei permessi personali oltre a quelli del gruppo a cui appartiene, il permesso che ne conseguirà sarà la somma di tutti, sia quelli personali che quelli di gruppo. Nell'esempio seguente l'UtenteA possiede il permesso di lettura sui file, oltre al permesso di scrittura ereditato dal GruppoA di appartenenza, e di divieto di scrittura sul FILE 2 ereditata dal GruppoB. Il risultato è che l'UtenteA potrà leggere e scrivere sul FILE 1 ma non avrà accesso al FILE 2.



Zoom su...

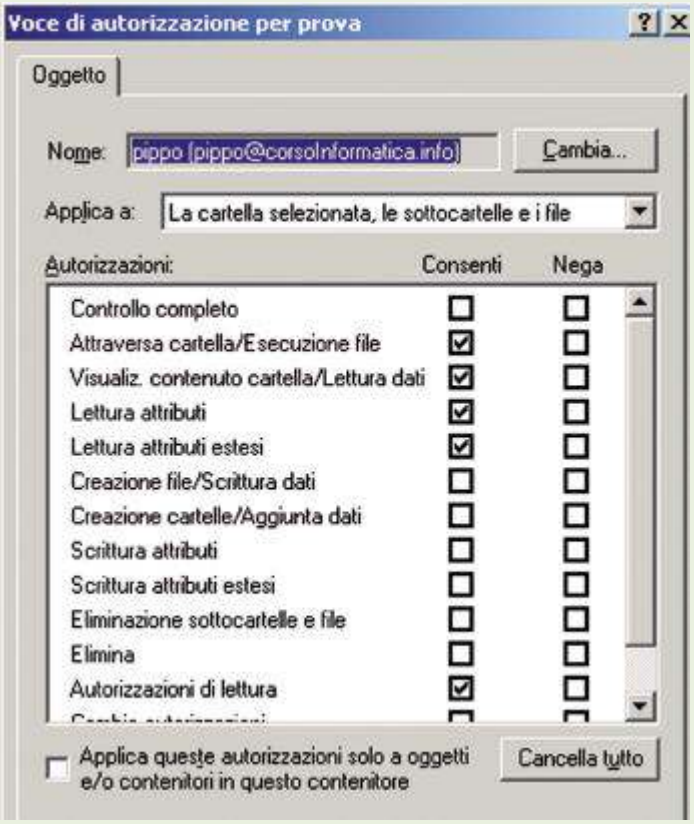
I PERMESSI SPECIALI

Esistono anche dei permessi speciali che permettono una selezione ulteriore delle autorizzazioni per cartelle e file. La loro combinazione ci riporta comunque ai permessi standard. Dopo aver creato una cartella (prova) facciamo clic su di essa con il tasto destro e selezioniamo Proprietà, quindi sulla scheda Protezione selezioniamo l'utente a cui assegnare i permessi su questa risorsa, in questo caso pippo:



Facendo clic sul pulsante Avanzate otteniamo la seguente finestra:

Facendo clic su Modifica otteniamo l'elenco completo di tutte le autorizzazioni assegnabili a questo utente:

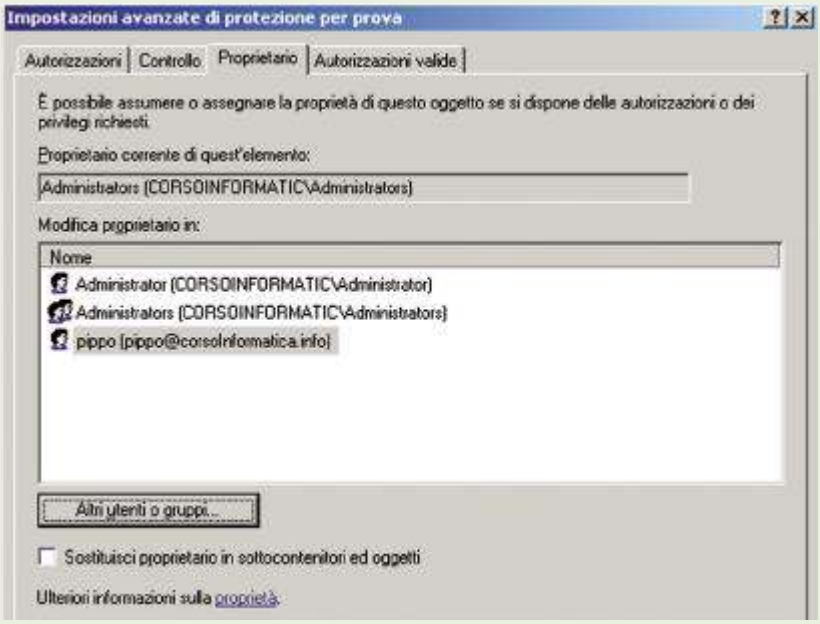


Analizziamole.

- Controllo Completo. Come visto in precedenza si tratta dell'insieme di tutti i permessi.
- Attraversa Cartelle/Esecuzione File. Permette di navigare nella directory ed eseguirne i file contenuti in essa.
- Visualizzazione contenuto cartella/Lettura dati. Consente di visualizzare il contenuto di una directory o di leggerne i file.
- Lettura Attributi. Permette di visualizzare le proprietà di un file o di una sottocartella.
- Lettura Attributi estesi. Permette di visualizzare le proprietà estese di un file o di una sottocartella.
- Creazione file/Scrittura dati. Permette di creare file all'interno di una cartella e di scriverci al suo interno.
- Creazione cartelle/Aggiunta dati. Consente di creare nuove sottocartelle o di aggiungere dati a un file.
- Scrittura attributi. Consente di modificare gli attributi di un file.
- Scrittura attributi estesi. Consente di impostare gli attributi estesi su file o cartelle.
- Eliminazione sottocartelle e file. Si applica solo alle cartelle e consente di cancellarne tutti gli oggetti contenuti in esse.
- Elimina. Consente di eliminare la cartella.
- Autorizzazioni di lettura. Consente di leggere le autorizzazioni di un file.
- Cambia autorizzazioni. Consente la modifica le ACL.
- Diventa proprietario. Consente di ottenere la proprietà di un oggetto, inoltre il proprietario può sempre modificare le ACL degli oggetti.

Come abbiamo detto in precedenza l'utente che crea un file ne è anche il Proprietario (Owner) ed è l'unico utente, oltre agli utenti del gruppo Administrators, con il diritto di impostarne le autorizzazioni. La proprietà può essere modificata in due modi:

- il proprietario corrente può concedere l'autorizzazione speciale Diventa proprietario al nuovo proprietario che potrà assumerla in qualsiasi momento;
- un amministratore può diventare proprietario dell'oggetto in qualsiasi momento attraverso la scheda proprietario che può essere ottenuta dalle Impostazioni avanzate, quindi scheda Proprietario:



I permessi di condivisione

I permessi di condivisione sono attribuibili a singoli utenti o a gruppi e sono riferiti solo a cartelle remote, accessibili dalla rete. Quindi per rendere accessibili le cartelle da parte di utenti da postazioni remote dovremo necessariamente renderle condivise. I permessi di condivisione non hanno alcun valore negli accessi locali.

Possiamo condividere le cartelle anche nei volumi FAT, oltre che NTFS. Nel caso di volumi NTFS per avere accesso da rete l'utente deve anche possederne i relativi permessi.

I permessi di condivisione sono sintetizzabili in:

- controllo completo
- modifica
- lettura

I permessi di condivisione sono cumulativi, per cui il permesso complessivo deriva dalla somma dei permessi dell'utente e del gruppo a cui appartiene. Fa eccezione il permesso di negazione che come spesso accade sovrasta tutti gli altri permessi.
Vediamo come procedere per condividere una cartella in rete: facciamo clic su di essa con il pulsante destro, quindi Proprietà e la scheda Condivisione. ▶

Il pulsante Autorizzazioni mostra gli utenti. ▶

In questo caso notiamo che il gruppo Everyone (insieme di tutti gli utenti) possiede il solo permesso di lettura.

Verifichiamo le conoscenze

1. Completamento

1 ..... è il database integrato nei sistemi operativi Windows Server che svolge il compito di .....

2 I criteri di gruppo hanno la funzione di semplificare il controllo decentralizzato su ....., ... e ..... di utenti e computer di un dominio.

3 I criteri di gruppo possono essere applicati a:

- .....
- .....
- .....
- .....
- .....

4 I permessi ..... possono essere utilizzati per limitare l'accesso a Internet a certi utenti.

5 Attraverso il file system NTFS possiamo specificare particolari permessi di accesso per le cartelle e per i singoli file a ..... o a .....

6 La strategia AGDLP, prevede i seguenti passi:

A) definire gli .....;

G) collocarli nei .....;

DL) poi dobbiamo inserirli nei .....;

P) infine dobbiamo assegnarne i ..... per l'accesso alle risorse.

7 NTFS consente di associare a ogni file o cartella una ..... contenente gli utenti e i gruppi che possono accedere alla risorsa e i relativi permessi.

8 L'..... di ciascuna risorsa deve contenere almeno un'Access Control Entry (ACE) associata a un utente o a un gruppo in modo da concederne l'accesso.

9 In relazione ai permessi NTFS sulle cartelle abbiamo che ..... consente di creare nuovi file e sottocartelle all'interno della directory, mentre ..... permette di visualizzare i nomi dei file e delle sottocartelle della directory.

10 In relazione ai permessi NTFS sui file, è noto che ..... consente di visualizzare i file con i relativi attributi, le proprietà e i permessi e ..... consente di creare nuovi file, cambiarne gli attributi, oltre a visualizzarne i permessi e le proprietà.

11 I permessi ..... sono attribuibili a singoli utenti o a gruppi e sono riferiti solo a cartelle remote, accessibili dalla rete.

12 I permessi di condivisione sono di tre tipi: ....., ... e .....

2. Vero o falso

1 Attraverso i criteri di gruppo si definiscono le procedure per gestire la sicurezza nel proprio ambiente. V F

2 I criteri di gruppo non possono essere applicati ai domini. V F

3 I criteri di gruppo locali vengono applicati prima dei criteri di gruppo di dominio. V F

4 I permessi NTFS vengono rilasciati secondo la policy chiamata AGDLP. V F

5 Il permesso NTFS Modify, per le cartelle permette la cancellazione della directory ma non i permessi Write e Read & Execute. V F

6 Il permesso NTFS Read & Execute, per i file consente di caricare le applicazioni, oltre a effettuare le azioni concesse da Read. V F

7 Per poter assegnare permessi NTFS a un file o a una cartella dobbiamo appartenere al gruppo Administrators. V F

LEZIONE 5

Il troubleshooting

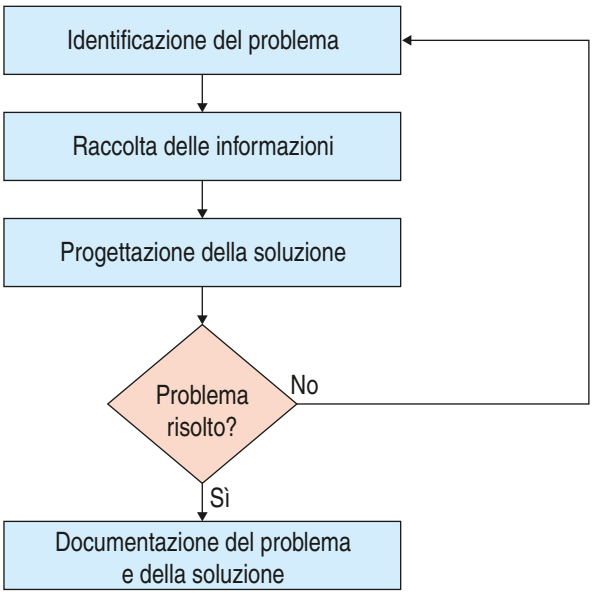
In questa lezione impareremo...

- a identificare e documentare i problemi di una rete
- i principali diagrammi di flusso che articolano il troubleshooting di una rete
- ad analizzare il lato client e server

Schema di troubleshooting

Le reti di comunicazione sono oggetti complessi, composti da un insieme interconesso di apparati hardware e software tramite i quali vengono forniti servizi agli utenti.

Quando all'interno di un sistema complesso come una rete di comunicazione si verifica un problema, dobbiamo necessariamente identificarlo seguendo uno schema logico così strutturato: ▶



La ricerca del problema del sistema e la sua soluzione, unitamente alla produzione della documentazione che ne illustra la soluzione, viene chiamata ◀ **troubleshooting** ▶ della rete.

◀ Troubleshooting significa eliminazione del problema ed è il processo che ricerca in modo sistematico e articolato le cause di un problema verificatosi alla rete interessata. Lo scopo del troubleshooting è risolverlo affinché il sistema sia operativo. ▶

È bene in genere verificare preliminarmente se il problema sussista effettivamente oppure no, in quanto capita che un utente non esperto associ la non fruizione di un servizio di rete come un problema di connettività, come ad esempio: “non riesco a scaricare la posta elettronica”, “non riesco a stampare”, “non riesco a visualizzare correttamente un sito Web”. Se infatti l’utente riesce a navigare ma non a scaricare la posta significa magari soltanto che il programma di posta elettronica non è stato configurato correttamente oppure che è momentaneamente indisponibile il server di posta. Spesso invece quando sono più servizi a non essere utilizzabili allora è possibile che siamo davanti a un problema effettivo di rete.

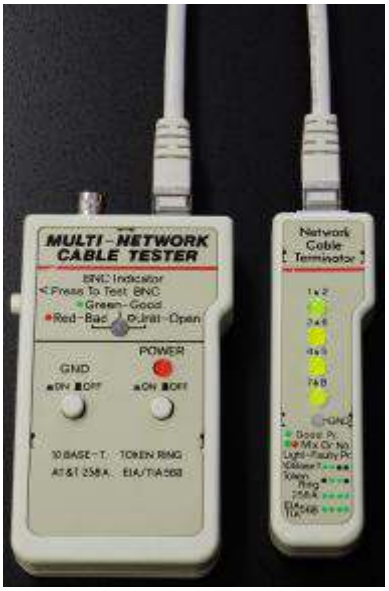
Controllo fisico

Una volta accertato che si tratti di un problema di rete, occorre effettuare alcune verifiche che possono risultare ovvie, ma che spesso possono portare alla risoluzione:

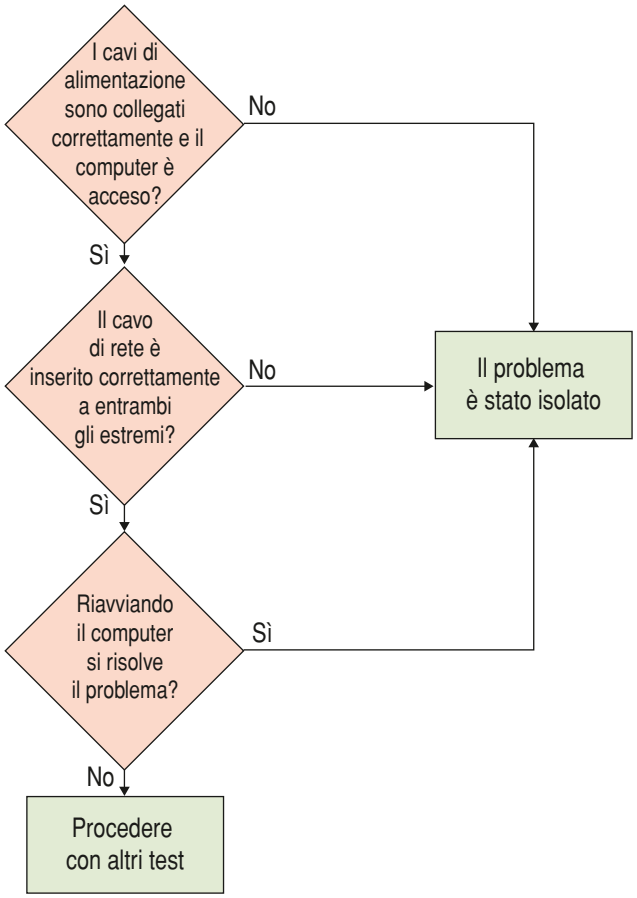
- controllare l’alimentazione: verificare che tutti i cavi di alimentazione siano collegati alle prese della rete elettrica e che il computer sia stato acceso;
- controllare la connettività: verificare che il cavo di rete sia connesso effettivamente e soprattutto saldamente alla scheda di rete e alla presa a muro. Se il cavo connesso alla scheda di rete è di tipo twisted pair, conviene estrarlo e reinserirlo fino a sentire il tipico clic che si ha quando raggiunge la corretta posizione.

A volte è bene anche verificare le polarità dei cavi presenti e la corretta posizione dei colori sul terminale RJ45, oltre a verificare che sia effettivamente di rete e non un cavo telefonico, che è simile, ma che possiede un connettore più stretto (RJ11).

Verificare che il LED presente nella scheda di rete sia acceso. Infine è utile verificare la connettività del cavo di rete utilizzato attraverso un LAN cable tester:



- **Riavviare il computer**: provare a riavviare il computer, a volte la nuova inizializzazione del sistema Operativo assegna le corrette impostazioni alla scheda di rete.
  La sequenza di operazioni da seguire in questa fase preliminare è riassunta nel successivo diagramma di flusso. Se, una volta eseguite queste verifiche, il problema non si risolve allora occorre procedere con altri test più dettagliati che vadano a isolare l'ambito in cui questo risiede.

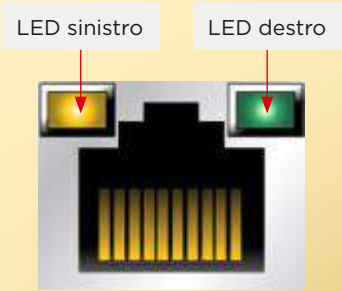


Scambio di componenti di rete

Le schede di rete (NIC Network Interface Card) possiedono dei particolari ◀ LED ▶ che indicano lo stato della connessione. Un LED spento indica chiaramente un problema di connettività tra la scheda e lo switch a cui è connesso il cavo.

La maggior parte delle porte Ethernet possiedono due LED, come mostrato nell'immagine e nella tabella descrittiva posta di seguito.

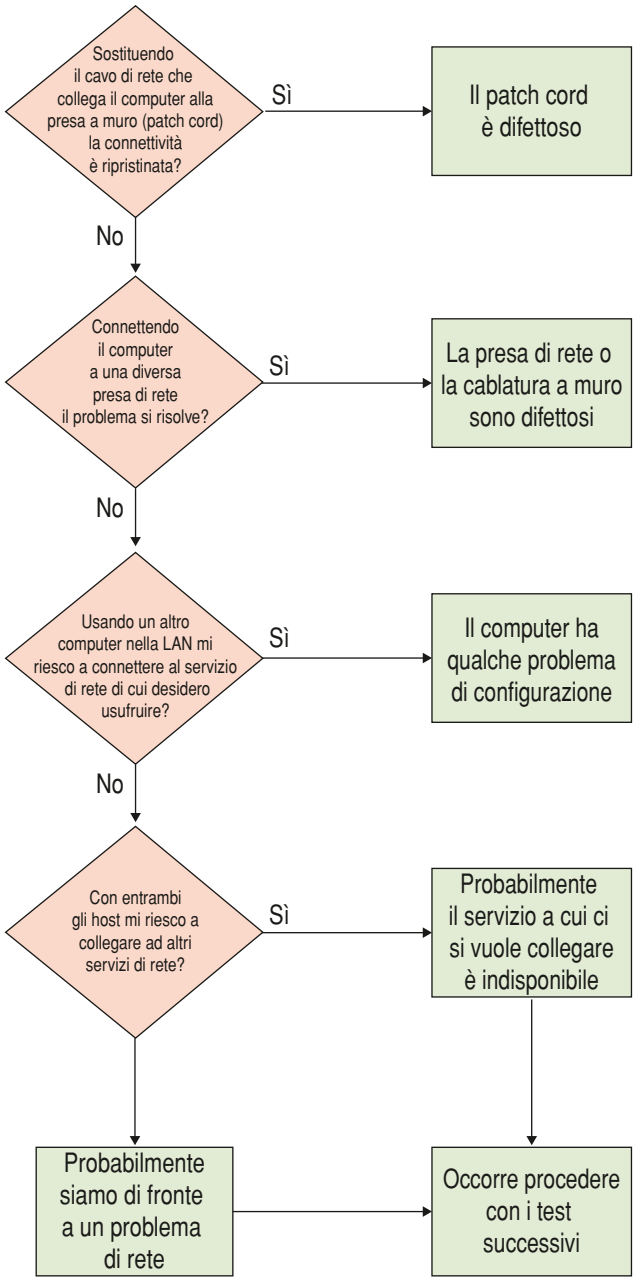
LED	Colore	Descrizione
LED sinistro	Giallo	Indicatore Link/Activity: Acceso: collegamento stabilito Lampeggiante: indica attività sulla porta Spento: nessun collegamento stabilito
LED destro	Giallo o Verde	Indicatore di velocità: Giallo: la connessione Gigabit è operativa (1000 Mbps) Verde: la connessione è operativa a 100 Mbps Spento: la connessione è operativa a 10/100 Mbps



Nel caso di LED spento occorre procedere con le successive operazioni necessarie a isolare il problema:

- sostituiamo il cavo patch che connette la scheda alla presa a muro con un altro: se il LED si accende e il computer riacquista tutte le funzionalità nell'uso della rete, significa che il problema era dovuto al cavo; se invece il LED non si accende ed è presente un'altra presa di rete vicina alla prima, allora si può passare alla fase successiva;
- colleghiamo il computer a un altra presa di rete: se la connettività di rete si attiva significa che il problema era evidentemente legato a difetti della prima presa di rete o della cablatura che la collega all'apparato di rete corrispondente; se invece la connettività non è ancora stabilita, il problema potrebbe risiedere nell'host stesso oppure potremmo essere di fronte effettivamente a un malfunzionamento della rete. Passiamo in tal caso a effettuare ulteriori verifiche;
- per verificare se il problema è della rete o del solo host visto sopra verifichiamo la connessione da un altro host della rete; se quest'ultimo si connette significa che probabilmente il problema risiede sull'host dell'utente e non sulla rete; se invece entrambi gli host non riescono a connettersi allo stesso servizio di rete, mentre ciò non avviene con altri servizi di rete, allora il problema potrebbe risiedere sul server.

Se entrambi gli host non accedono ai servizi di rete, probabilmente si tratta di un effettivo malfunzionamento della rete, dobbiamo quindi procedere a ulteriori controlli. Prima di tutto dobbiamo verificare se il problema è nel client dell'utente oppure sul server che lo fornisce. Un'altra causa potrebbe essere legata a un malfunzionamento del DNS (Domain Name System) o a un punto intermedio tra client e server. Il seguente flow chart riassume le operazioni che abbiamo appena descritto. ▶



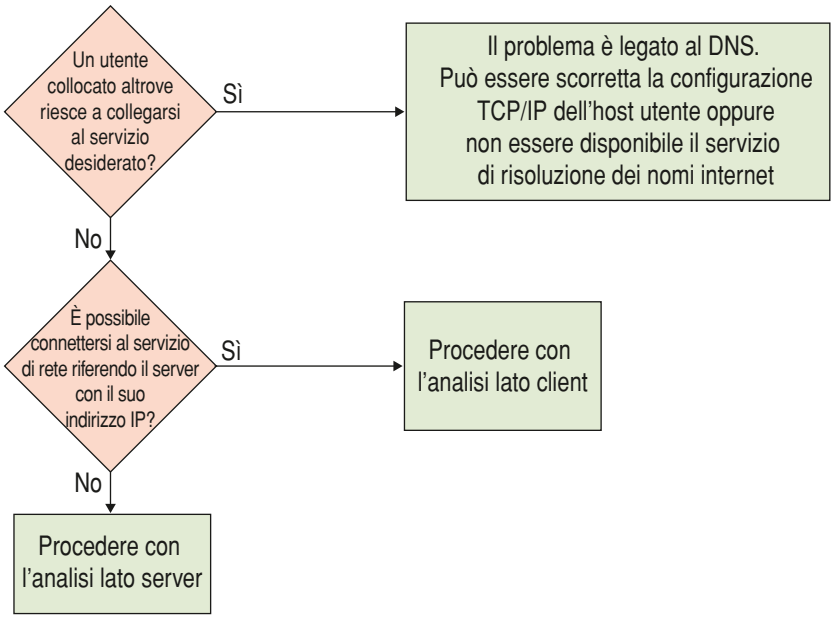
Verifica della connettività TCP/IP

La verifica della connettività TCP/IP analizza la fruibilità dei servizi di rete come ad esempio Web, mail, FTP, telnet ecc.
Supponiamo di voler effettuare una connessione a un host mediante protocollo TCP/IP, ad esempio all'URL di un Web server, si potrebbero verificare due casi distinti di errore:

- se otteniamo il tipico messaggio (Errore 404 – pagina non trovata) significa che la rete funziona correttamente, il problema in questo caso risiede sul server;
- se invece otteniamo un messaggio di errore del tipo il server non esiste o non posso trovare il server allora siamo di fronte a un possibile problema di rete;
- se invece il server risulta raggiungibile mediante l'indicazione del solo indirizzo IP di destinazione allora siamo di fronte a uno dei seguenti problemi di DNS:
  – potrebbero essere sbagliati i riferimenti ai DNS server nella configurazione di rete dell'host;
  – che manifesta il malfunzionamento;
  – potrebbe esserci un problema sui DNS server oppure potrebbero non essere raggiungibili.

Possiamo anche verificare, collegandoci al server da una diversa locazione:
- se la connessione ha successo allora il problema si trova lato client;
- se la connessione fallisce allora il problema è legato alla rete o si trova lato server.

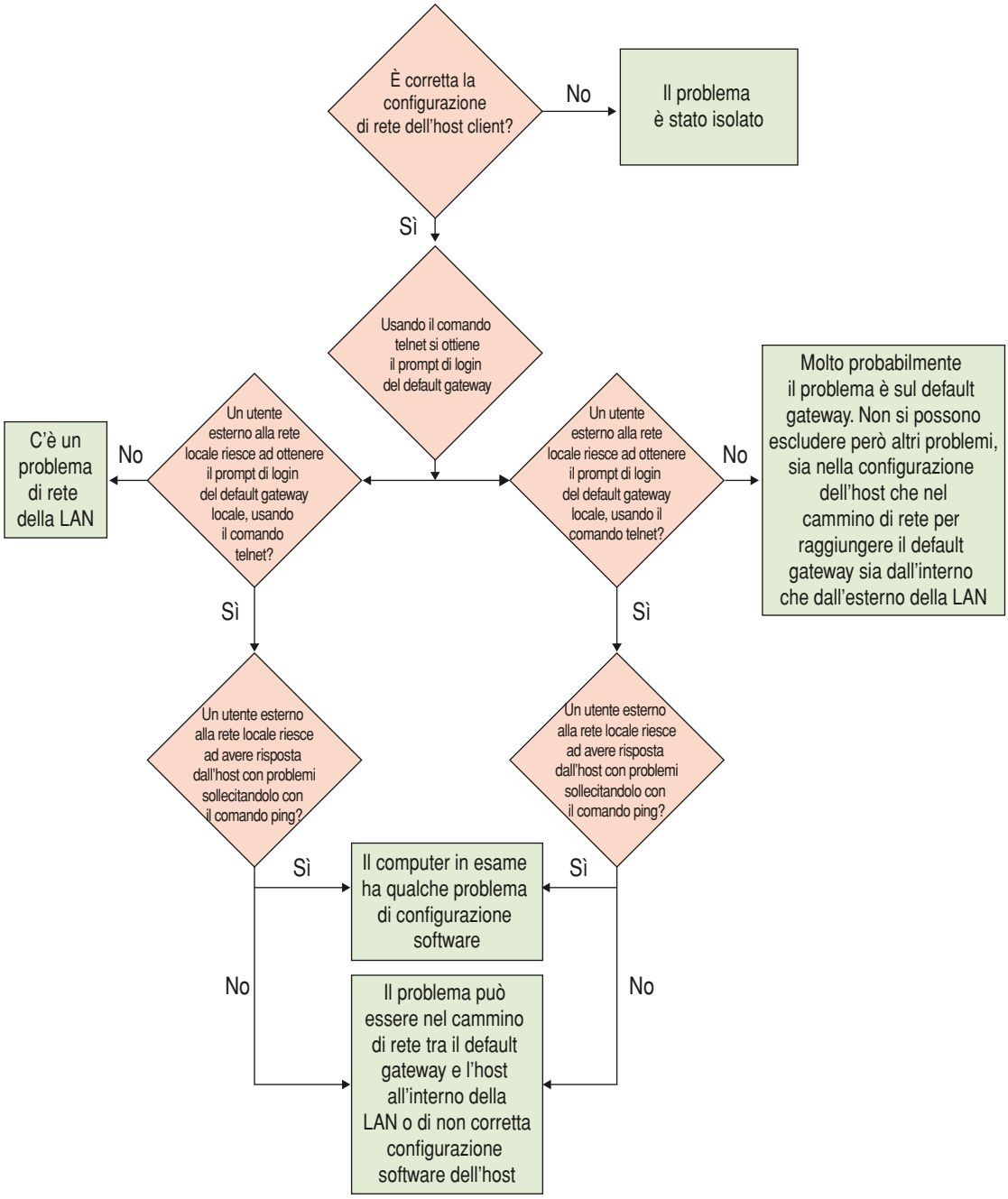
Il diagramma di flusso che descrive questa procedura è riportato di seguito.



Analisi lato client

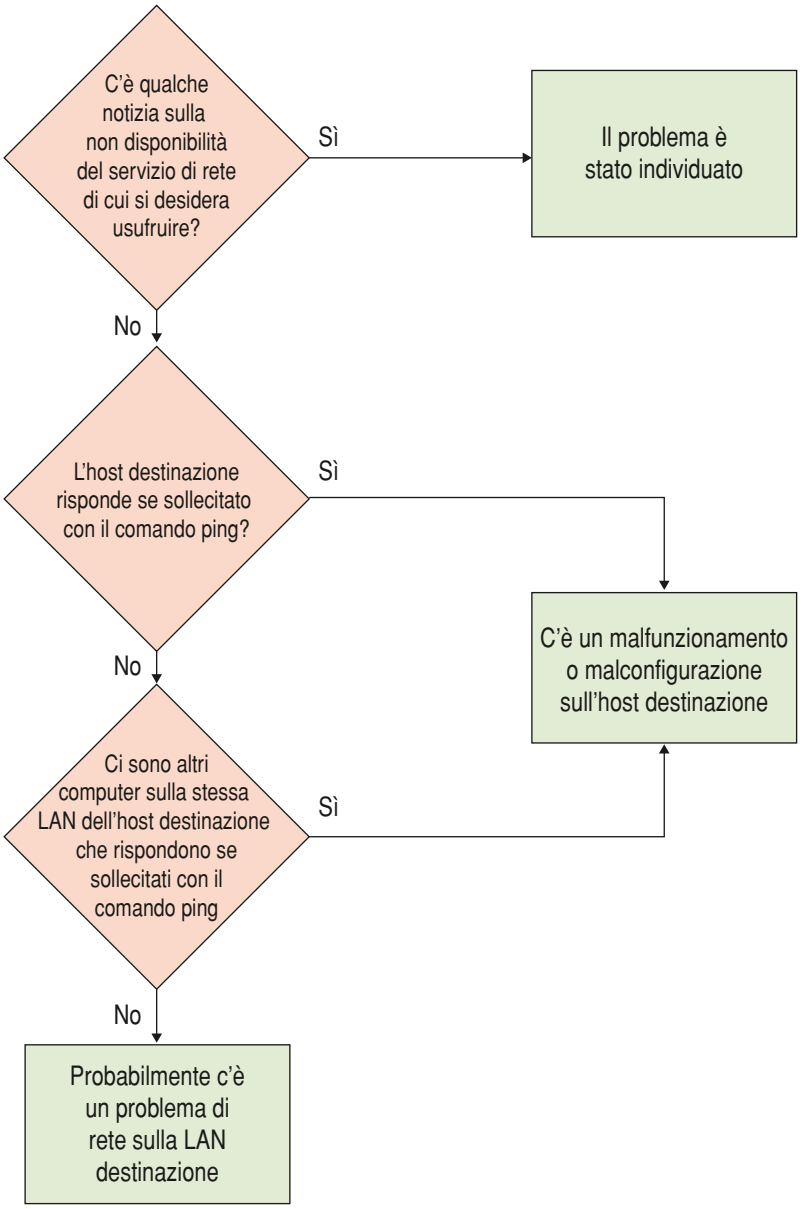
La verifica che dobbiamo effettuare sul client per prima cosa deve tenere conto della configurazione di rete dell'host, rappresentata dall'indirizzo IP, subnet mask, default gateway. Dopo aver verificato questi dati passiamo alla verifica del default gateway. Possiamo utilizzare il comando telnet da linea di comando per verificare l'indirizzo IP del gateway, se otteniamo in risposta la login del router allora molto probabilmente la nostra configurazione di rete è corretta e il malfunzionamento è dovuto a un problema di rete posto in un punto successivo al router.

Se invece non riusciamo a connetterci al default gateway, allora potrebbe esserci un problema sul router o su un'apparecchiatura di rete intermedia. In quest'ultimo caso sarebbe utile provare la connessione all'esterno del router da un host diverso della rete, sempre attraverso il comando telnet. Nel caso in cui l'operazione fallisca il problema può essere legato al router o al cammino di rete per raggiungerlo. Se l'operazione ha successo possiamo provare a sollecitare dall'esterno, attraverso il comando ping, l'indirizzo IP dell'host con i problemi visti in precedenza. Se l'host in questo caso risponde, significa che il software sull'host non è configurato correttamente, in caso contrario non si può escludere che sia un problema legato al cammino di rete tra il default gateway e l'host stesso. Infine riportiamo il flow chart del percorso logico seguito.



Analisi lato server (a livello applicazione)

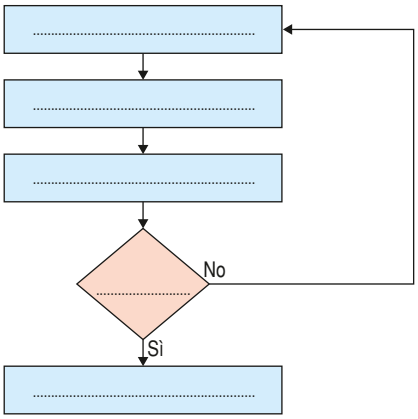
Quando giungiamo a questo punto dell'analisi del problema significa che, molto probabilmente, il problema risiede nella rete di destinazione. La prima cosa da fare è escludere che il servizio richiesto sia per qualche motivo attualmente non disponibile. In caso contrario potremmo provare a pingare l'indirizzo IP dell'host destinazione. Se si verifica la connessione tra i due host significa che il problema appartiene a quest'ultimo. Se invece le due macchine non si pingano (esito del ping negativo) possiamo sollecitare, mediante un'applicazione per lo scanning di rete, IP diversi da quelli della macchina destinazione. Se l'operazione ha successo, significa che abbiamo individuato host diversi da quello destinazione che rispondono al comando ping e che risiedono sempre sulla stessa LAN di quest'ultimo; in questo caso il problema consiste in qualche malfunzionamento o non corretta configurazione della macchina destinazione, in caso contrario non si può escludere un problema nella rete target. Il flow chart che sintetizza questa procedura è il seguente:



Verifichiamo le conoscenze

1. Completamento

1 Riempi le parti mancanti nello schema seguente secondo la tecnica di troubleshooting che hai appreso:



2 Secondo il controllo fisico dobbiamo prima di tutto ....., quindi ..... attraverso il cavo di rete, quindi se è il caso .....

3 Nella scheda di rete quando il LED di destra è di colore giallo significa che la connettività è di ....., se è di colore verde ....., se è spento .....

4 Nella scheda di rete quando il LED di sinistra è acceso significa che ....., se lampeggia significa che ....., se infine è spento significa che .....

5 Per verificare la connettività TCP/IP, facendo un collegamento al server da ....., se la connessione ha successo allora il problema si trova ....., invece se la connessione fallisce allora il problema è legato .....

6 La prima verifica da fare sul client è relativa alla ..... dell'host, rappresentata dall'indirizzo IP, subnet mask e default gateway.

7 Attraverso un comando ..... si può verificare l'indirizzo IP del gateway, se si ottiene come risposta ..... significa che il problema è posto in un punto successivo al router.

8 Se il server è raggiungibile mediante l'indicazione del solo indirizzo IP di destinazione allora il problema è la scorretta ..... oppure .....

9 Se usando il comando telnet si ottiene il prompt di login del default gateway e un utente esterno alla rete locale riesce a ottenere il prompt di login del default gateway locale, usando il comando telnet e infine un utente esterno alla rete locale riesce ad avere risposta dall'host con problemi sollecitandolo con il comando ping?, significa che il computer locale ha dei problemi di .....

2. Ordinamento

1 Metti in ordine logico le seguenti operazioni che determinano il problema relativo allo stato della connessione:

- ..... Connettere il computer a una diversa presa di rete.
- ..... Con entrambi gli host mi riesco a collegare ad altri servizi di rete.
- ..... Sostituire il cavo di rete che collega il computer alla presa a muro.
- ..... Usare un altro computer nella LAN.

LEZIONE 6

La sicurezza della rete

In questa lezione impareremo...

- da cosa e da chi proteggere il sistema
- a riconoscere i livelli di sicurezza da intraprendere
- a conoscere i principali tipi di attacco
- ad adottare sistemi di monitoraggio e di disaster recovery

Reti sicure

Per rendere sicura una rete dobbiamo conoscere sia le opportune misure da intraprendere che conoscere da chi o da cosa proteggere il sistema. Iniziamo a vedere da cosa dobbiamo proteggerci:

- Hacker: si tratta di un individuo o un gruppo di individui il cui obiettivo è accedere nei sistemi per diversi motivi che vanno dal puro divertimento, allo studio, alla curiosità o semplicemente per dimostrare di essere in grado di farlo. Nella maggior parte dei casi l'hacker non causa gravi danni al sistema della vittima.
- Cracker: si tratta di un individuo o di un gruppo di individui il cui obiettivo è violare i sistemi di sicurezza informatici per provocare un danno. Si possono dividere in due tipi:
  – Outsiders: sono coloro che operano dall'esterno del network che intendono attaccare;
  – Insiders: sono coloro che sono autorizzati all'uso della rete e che cercano di abusarne.

La sicurezza della rete è definita dal livello di ◀ fault tolerance ▶ della stessa rete.
Una rete non può essere considerata una struttura poco sicura, a motivo sia della sua struttura fisica che logica, inoltre per una azienda i malfunzionamenti sono causa di guai e di conseguenza di costi aggiuntivi. Nelle reti di grandi dimensioni la funzionalità della rete deve essere garantita con bassissimi margini di errore, per raggiungere questo risultato tuttavia le soluzioni sono complesse. Una rete può essere soggetta, come abbiamo visto nella scorsa lezione, a malfunzionamenti di vario genere, basti pensare che ad esempio un problema ai server di un noto ISP ha bloccato migliaia di siti Web. Per ridurre il rischio di blocchi della rete dobbiamo utilizzare le seguenti strategie:

◀ Fault tolerance è la capacità di un sistema di eseguire normalmente le operazioni malgrado la presenza di errori hardware o software. ▶

- bloccare i tentativi di intrusione dall'esterno;
- proteggere la rete da attività di utenti che possono compiere atti dolosi o colposi;
- utilizzare sistemi di controllo e di monitoraggio della rete;
- ampliare il livello di affidabilità e di sicurezza attraverso sistemi di controllo dell'alimentazione, degli impianti, dei locali, e delle strutture che li ospitano;
- utilizzare le tecniche di ridondanza di server e servizi.

Un atto o evento che tende a violare la sicurezza delle informazioni trasmesse all'interno della rete, prende il nome di procedura di attacco. Gli attacchi alla sicurezza della rete si possono classificare secondo due grandi categorie:
- minacce attive: in cui l'entità non autorizzata accede alle informazioni e le altera o le ritrasmette in modo da trasmettere informazioni false;
- minacce passive: vengono anche chiamate intercettazioni e rappresentano i tentativi da parte di terzi di accedere alle informazioni trasmesse durante una comunicazione.

Quindi possiamo comprendere che l'implementazione di tecniche di protezione e la definizione dei servizi coinvolge in effetti l'intera architettura di rete. Dobbiamo quindi capire in quale modo i protocolli agiscano rispetto alla protezione dei dati. I sistemi di sicurezza specifici per la rete considerata devono prevedere un'analisi dettagliata dei rischi al fine di poter individuare la tecnica migliore sia dal punto di vista dell'efficienza che dal punto di vista economico. Inoltre, la conoscenza delle tecniche d'attacco consente all'amministratore di sistema di proteggere i propri sistemi prevenendo gli attacchi, ovvero adottando le misure necessarie a ridurre i fattori di rischio di esposizione.

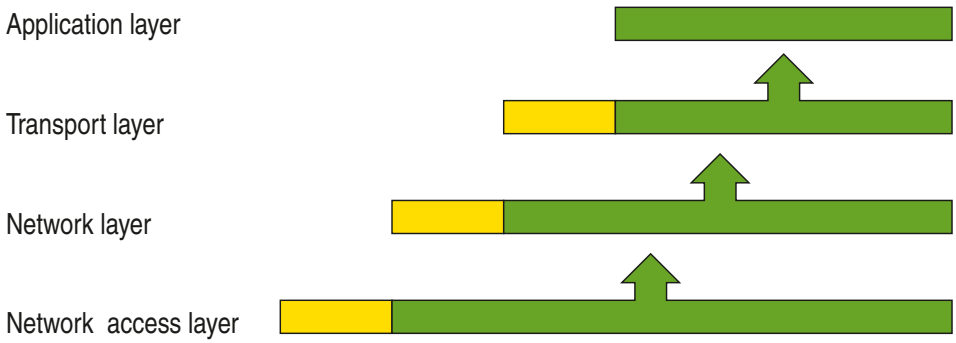
Adesso concentriamoci sui servizi principali offerti da Internet per capire quali siano i loro principali problemi di sicurezza. Un servizio è sicuro quando garantisce che:
- non può essere utilizzato per operazioni diverse da quelle previste;
- non si possa leggere e/o falsificare le transazioni che avvengo attraverso il servizio stesso. Tali garanzie non implicano che si possano eseguire transazioni con il servizio continuando a essere al sicuro. Per esempio, si potrebbe utilizzare un HTTP (HyperText Transfer Protocol) sicuro per effettuare il download di un file, ed essere sicuri che si stia effettivamente effettuando il download del file a cui si è interessati, e che nessuno lo stia modificando nel transito. Ma non si possono avere garanzie che il file non contenga dei virus o programmi dannosi.

> È possibile anche utilizzare servizi insicuri in modo sicuro, ma ciò richiede maggiore cautela. Ad esempio, la posta elettronica attraverso il protocollo SMTP (Simple Mail Transfer Protocol) è un classico esempio di un servizio insicuro.

Sicurezza nei protocolli TCP/IP

I firewall utilizzano tecniche di packet filtering per difendere la propria rete; a tal proposito rivediamo gli strati software che costituiscono l'architettura TCP/IP:
- Application Layer (FTP, HTTP, DNS, POP3 ecc.);
- Transport Layer (TCP o UDP);
- Internet Layer (IP).

A ogni livello un pacchetto si compone di due parti chiamate intestazione (header) e dati (payload). L'intestazione contiene informazioni rilevanti per il protocollo, mentre il payload contiene i dati, come sappiamo la costruzione del pacchetto avviene in base al meccanismo che prevede che ciascuno strato aggiunga proprie informazioni di controllo al campo dati ricevuto dallo strato soprastante. Questo procedimento che consiste nel ricevere un pacchetto da un protocollo di livello superiore e nell'aggiungere a tale pacchetto una propria intestazione viene detto incapsulamento.



I pacchetti IP possono essere di tipo unicast, cioè vengono spediti verso un unico host di destinazione, multicast, cioè spediti a un gruppo di host oppure broadcast, cioè indirizzati a tutti gli host che possono riceverli nell'ambito della rete logica di appartenenza del mittente. Gli indirizzi di multicast e di broadcast sono indirizzi di destinazione e non di origine, altrimenti potrebbero essere utilizzati da una procedura di attacco che utilizzerebbe una macchina di destinazione per amplificare l'attacco. Un firewall quindi deve rifiutare i pacchetti destinati a un indirizzo di broadcast e i pacchetti il cui indirizzo di origine sia un multicast o un broadcast.

L'intestazione del pacchetto IP include un campo Options che è stato progettato per utilizzare informazioni speciali come ad esempio i tentativi di attacco. La più comune opzione IP che un firewall è costretto a controllare è l'opzione di source routing.

Questa opzione, presente in alcuni pacchetti, consente al mittente del pacchetto di specificare il percorso che il pacchetto dovrebbe seguire per giungere a destinazione, piuttosto che consentire a ogni router lungo il cammino di usare la propria routing table per decidere a quale router successivo consegnare il pacchetto.
Il source routing è stato progettato per sovrascrivere le istruzioni presenti nelle routing table. Lo scopo del source routing è di aggirare i router che possiedono routing table guaste o non corrette. In pratica, il source routing viene comunemente utilizzato solamente dagli attaccanti che tentano di aggirare le misure di sicurezza costringendo i pacchetti a seguire cammini inaspettati. Alcuni sistemi di protezione seguono l'approccio di scartare tutti quei pacchetti che hanno le opzioni IP impostate, senza nemmeno analizzarle.

Una delle caratteristiche del protocollo IP è la sua capacità di dividere un pacchetto di grandi dimensioni, che altrimenti non potrebbe attraversare una rete, in pacchetti più piccoli chiamati frammenti, che possono attraversare la rete per essere riassemblati nell'host di destinazione.
Qualunque router può decidere di frammentare un pacchetto, anche se un campo posto nell'intestazione IP può essere utilizzato per evitare che un router frammenti un pacchetto. Tale campo viene utilizzato per conoscere la MTU (Maximun Transmission Unit) attraverso una tecnica che determina quale sia il pacchetto più grande che possa essere inviato a un host senza subire la frammentazione.
Il problema è che il firewall verifica solo il primo frammento, perché è in tale frammento che vi sono memorizzate le informazioni testabili. Il primo frammento infatti contiene informazioni relative ai protocolli di alto livello, in base a quel frammento il firewall deciderà se far passare o meno il pacchetto. Una tecnica prevede di consentire il passaggio a tutti i frammenti facendo il controllo solamente sul primo, se il firewall decide di scartarlo, il pacchetto originale non può essere ricostruito, in quanto il pacchetto parzialmente riassemblato non può essere accettato dall'host.
Consentire il passaggio a tutti i pacchetti eccetto il primo è comunque rischioso in quanto l'host di destinazione manterrebbe i frammenti non scartati in memoria per un certo periodo, in attesa di ricevere il pezzo mancante. Questo esporrebbe il sistema a un rischio terribile: l'attaccante potrebbe usare i pacchetti frammentati rimasti in memoria per sferrare un attacco di tipo ◀ DoS ▶.

◀ Un attacco DoS (Denial of Service) ha lo scopo di ottenere l'esaurimento delle risorse di un sistema che fornisce un servizio, come ad esempio un Web server, fino a renderlo non più in grado di erogare il servizio. Gli attacchi vengono abitualmente attuati inviando molti pacchetti di richieste, di solito a un Web server, FTP o di posta elettronica saturandone le risorse e rendendolo instabile. Attualmente gli attacchi DoS sono spesso di tipo criminale, in quanto tentano di impedire agli utenti della rete l'accesso ai siti Web vittime dell'attacco. Per rendere più efficace l'attacco in genere vengono utilizzati molti computer inconsapevoli, detti zombie, sui quali precedentemente è stato inoculato un programma appositamente creato per attacchi DoS e che si attiva a un comando proveniente dal cracker creatore. Quando il programma maligno è diffuso su molti computer, chiamati botnet, essi produrranno un flusso incontenibile di dati che travolgeranno come una valanga anche i link più capienti del sito bersaglio. ▶

In questo tipo di attacco l'host di destinazione rinuncia ad assemblare un pacchetto, spedendo un messaggio ICMP di tipo packet reassembly time expired in risposta al mittente. Tale messaggio informerà così l'attaccante dell'esistenza dell'host e del motivo per cui il firewall non ha accettato il pacchetto.

I pacchetti frammentati rimasti in memoria dell'host destinazione possono anche essere usati dagli attaccanti per costruire pacchetti nelle parti in cui i frammenti si sovrappongono. Siccome un frammento sovrapposto non è normale spesso i sistemi operativi li riassemblano in pacchetti non validi che possono essere usati per tre tipologie di attacco:

- attacchi di tipo DoS contro sistemi che gestiscono male i frammenti che si sovrappongono;
- attacchi di tipo Information hiding, di fronte a sistemi che rilevano virus o intrusioni, vengono costruiti frammenti che nascondono il reale contenuto del pacchetto;
- attacchi che prelevano informazioni da servizi che non dovrebbero essere accessibili. Un "attaccante" costruisce un pacchetto con un'intestazione valida nel primo frammento e la sovrappone ai frammenti successivi, siccome il firewall non analizzerà le intestazioni dei frammenti successivi.

La soluzione che scarta tutti i frammenti è sicuramente più sicura anche se distruttiva perché distrugge anche connessioni "sane".

Protocollo TCP e sicurezza

Il protocollo TCP è bidirezionale, quando viene infatti stabilita una connessione client-server, quest'ultimo ha la possibilità di rispondere al client sulla stessa connessione.
Per bloccare una connessione TCP è sufficiente bloccare il primo pacchetto di tale connessione, cioè quello che contiene il campo SYN=1. Senza il primo pacchetto, qualunque altro pacchetto successivo al primo non potrà essere riassemblato sul lato ricevente. Qualunque altro pacchetto, successivo al SYN iniziale, indifferentemente dalla direzione in cui viaggia, è contraddistinto dal bit ACK=1.
Per le politiche di sicurezza è importante riconoscere i pacchetti di apertura della connessione, in quanto consente ai client interni di connettersi ai server esterni ma può vietare a client esterni di connettersi ai server interni. I campi presenti in un pacchetto TCP sono:

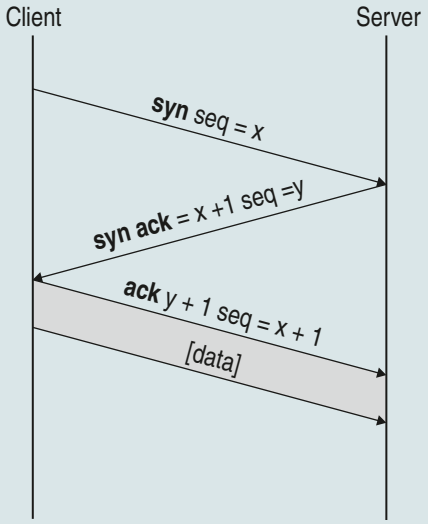
- URG (URGent);
- PSH (PuSH);
- ACK (ACKnowledgement);
- SYN (SYNchronize);
- FIN (FINish);
- RST (ReSeT).

I campi URG e PSH vengono utilizzati per identificare dati particolarmente critici, in particolare PSH comunica al ricevente di interrompere il buffering e consegnare i dati allo strato applicativo, mentre URG identifica i dati che il mittente considera genericamente importanti. In pratica entrambi possono essere trascurati dai firewall.
I campi ACK e SYN vengono utilizzati per implementare il protocollo Threeway Handshake. Il campo SYN è impostato a 1 nei primi due pacchetti che vengono utilizzati per stabilire una connessione.
I campi FIN e RST vengono utilizzati per chiudere le connessioni. Il campo RST viene utilizzato per una chiusura brutale, mentre FIN viene utilizzato per una chiusura concordata tra client e server.
Da questo si deduce che i campi ACK e RST devono essere verificati da un firewall in quanto:

- ACK consente di rilevare in maniera affidabile il primo pacchetto della connessione;
- RST fornisce un modo utile per chiudere una connessione senza dover spedire messaggi di errore.

Per poter ricostruire correttamente i pacchetti ricevuti, il protocollo TCP identifica i pacchetti attraverso un numero, chiamato numero di sequenza. Durante una connessione tra due host, ciascun host seleziona il numero di sequenza da cui iniziare lo scambio di pacchetti secondo il protocollo ◀ Threeway Handshake ▶.

◀ Threeway Handshake Nel momento in cui un client si connette a un server, il client invia una richiesta SYN, il server risponde quindi con un pacchetto SYN/ACK e infine il client convalida la connessione con un pacchetto ACK (acknowledgement) che identifica il riconoscimento e l'accettazione della richiesta. Una connessione TCP inizia quando queste tre tappe sono state concluse. ▶



L'attacco SYN consiste nell'inviare un gran numero di richieste SYN a un host con un indirizzo IP sorgente inesistente o non valido. In questo modo diventa impossibile per l'host bersaglio ricevere un pacchetto ACK. Gli host vulnerabili agli attacchi SYN mettono in lista d'attesa, in una struttura di dati in memoria, le connessioni aperte in attesa di ricevere un pacchetto ACK.

Esiste un meccanismo di scadenza che permette di rigettare i pacchetti dopo un certo periodo di tempo. Inoltre, raggiunto un numero elevato di pacchetti SYN, se le risorse utilizzate dal terminale per immagazzinare le richieste in attesa sono sature, questo rischia di diventare instabile fino ad arrivare al blocco o al riavvio.

Zoom su...

PROTEZIONE DA ATTIVITÀ DI UTENTI CHE POSSANO COMPIERE ATTI DOLOSI O COLPOSI

Spesso gli attacchi a una rete non provengono dall'esterno, ma da attività di utenti autorizzati all'interno della stessa rete. Le cause di malfunzionamenti di una rete, accertato che provengano da utenti interni, possono essere così classificate:

- cause colpose;
- cause dolose.

Le ◀ **cause colpose** ▶ sono dovute a imperizia di utenti inesperti o non ben preparati e sono le più diffuse. I danni ascrivibili a questa categoria di utenti vanno da danni minimi o irrisori, come ad esempio la cancellazione del profilo, a danni seri come ad esempio quando l'utente tenta di formattare una chiavetta estraibile e invece formatta un hard disk, oppure quando cancella file di sistema oppure ancora esegua le procedure di spegnimento in modo non corretto. Questi danni non dovrebbero comunque riguardare i server in quanto nella corretta gestione delle policies si esclude che utenti poco esperti abbiano accesso a risorse privilegiate di amministrazione della rete e dei servizi.

◀ Cause colpose La colpa sussiste quando l'autore del reato, pur agendo con volontà, non ha in alcun modo preso coscienza delle conseguenze della sua azione e, allo stesso tempo, l'evento si verifica a causa dell'imprudenza o imperizia dell'agente stesso, ovvero a causa della sua inosservanza di leggi, regolamenti, ordini o discipline. ▶

Le ◀ **cause dolose** ▶ si hanno quando avviene una manomissione volontaria delle postazioni di lavoro, sono assai poco diffuse ma tuttavia sono le più gravi in quanto implicano una volontà nella creazione di un danno. Tipici esempi sono l'installazione di software non autorizzato, modifica delle impostazioni di sistema oppure ancora di password o di materiale di riservato.

◀ Cause dolose Il dolo sussiste quando l'autore del reato agisce con volontà ed è cosciente delle conseguenze della sua azione o omissione. ▶

Sistemi di controllo e monitoraggio

Monitorare cosa accade all'interno di una rete (network auditing) unitamente al controllo delle informazioni che transitano attraverso i router ed i firewall incrementa la fault tolerance della rete stessa. Attraverso queste due tecniche possiamo risalire alle cause di un inconveniente o di un attacco ed eventualmente al responsabile. I server Windows dispongono di un sufficiente strumento di monitoraggio che consente l'auditing di ciò che avviene. Vediamo le principali operazioni che possono essere monitorate:

- eventi di accesso all'account;
- eventi di gestione dell'account;
- eventi di accesso a oggetti di Active Directory;
- eventi di accesso (logon);
- eventi di accesso a oggetti;
- eventi di modifica dei criteri (policies);
- eventi di uso dei privilegi;
- eventi di controllo dei processi;
- eventi di sistema.

AREA *digitale*

Impostare i criteri di auditing

Affidabilità e sicurezza delle strutture

Le strutture fisiche che ospitano la rete, quindi i locali e gli impianti di climatizzazione, alimentazione e cablaggio devono essere a norma di legge (decreto legislativo 9 aprile 2008 n. 81) per garantirne la sicurezza. È infatti insensato creare un sistema sicuro sotto tutti i punti di vista dal punto di vista software che venga magari compromesso da un allagamento oppure da un incendio.
Per ottimizzare la sicurezza fisica della struttura di una rete con server è pratica assai diffusa, oltre che sensata, quella di collocare il server in un'area accessibile solo a persone autorizzate. Inoltre dobbiamo posizionare i computer che ospitano i servizi di dominio in un luogo fisicamente protetto. La soluzione ideale è rappresentata da una sala computer chiusa, con monitoraggio e rilevamento di allagamenti e sistemi di rilevamento e spegnimento incendi. Inoltre è utile utilizzare un sistema che garantisca la continuità elettrica (◀ UPS ▶).

◀ UPS è l'acronimo di Uninterruptible Power Supply (gruppo di continuità), ovvero una apparecchiatura che si usa per mantenere costantemente alimentati elettricamente in corrente alternata apparecchi elettrici la cui funzionalità è essenziale per l'erogazione di un determinato servizio. ▶

La continuità elettrica rappresenta un elemento essenziale all'interno di una rete. È opportuno che tutti gli apparati di rete siano alimentati da una linea elettrica privilegiata e ciò sia al fine di garantirne la salvaguardia in caso di sbalzi di tensione, che potrebbero danneggiarli in maniera irreparabile, sia per garantire l'erogazione dei servizi in caso di black out.

Ridondanza di server e servizi

Il limite strutturale di una rete a dominio è che se il server non funziona tutte le attività a esso legate vengono evidentemente bloccate. Le procedure di sicurezza in questi casi possono prevedere l'attivazione di backup programmati dei server, la creazione di immagini dei dischi, l'uso di sistemi disco RAID (Redundant Array of Independent Disks) soprattutto in configurazione mirroring (RAID1) che prevede l'uso di due dischi o in configurazione RAID 0+1 con quattro dischi.

Nella configurazione RAID1 i dati vengono scritti in modo speculare su due dischi, per cui nel caso uno dei due si rompesse sarebbe sufficiente sostituirlo e ripristinare da quello superstite. La configurazione RAID0+1 prevede anche lo striping dei dati su due dischi che sono speculari ad altri due. In questo caso alla sicurezza del mirroring si aggiungono le maggiori performance in scrittura e lettura dello striping.

Quando in una rete prevediamo che un server sia sempre in funzione (24H), dobbiamo prevedere un secondo domain controller (DC) che lavori in load balancing con quello esistente, in modo da poter usare entrambi per l'autenticazione dell'utente e la distribuzione dei servizi essenziali alla rete come ad esempio DNS, WINS, DHCP. Nel caso che uno dei due sia temporaneamente bloccato, in seguito ad esempio a semplice manutenzione, l'altro consentirà comunque l'utilizzo dei servizi. La ridondanza dei servizi ha senso solo se questi sono replicati tra i due server, ad esempio la replica di Active Directory consente ai due server di gestire gli stessi utenti, gruppi, Unità Organizzative e computer.

Installazione di un server cluster

Un server cluster è un gruppo di sistemi indipendenti che lavorano insieme come un unico sistema: i client interagiscono con un cluster come se fosse costituito da un singolo server. Tale configurazione è utilizzata per incrementare sia la disponibilità che la scalabilità. Se un sistema in cluster fallisce, il software risponde reindirizzando il lavoro dal sistema bloccato all'altro sistema del cluster

(disponibilità), mentre se le richieste eccedono le capacità di risposta dei sistemi in cluster possiamo aggiungere altri server al cluster, aumentandone le capacità di eleborazione (scalabilità).

Piano di disaster recovery

Il piano di ◀ disaster recovery ▶ assicura, in caso di eventi disastrosi, la continuità delle operazioni indispensabili a fornire i servizi e il ritorno alla normale operatività.

◀ Disaster recovery Si tratta dell'insieme di misure tecnologiche e organizzative/logistiche atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business per imprese, associazioni o enti, a fronte di gravi emergenze che ne intacchino la regolare attività. ▶

L'integrità fisica dei sistemi informatici può essere messa a repentaglio da calamità naturali (fulmini, alluvioni, terremoti...), cause accidentali (incendi, allagamenti, crolli...) o cause esterne (furti, rivolte, devastazioni...). L'integrità delle infrastrutture necessarie al funzionamento dei sistemi possono essere messe a repentaglio da cali di elettricità, problemi di connettività di rete o difetti negli eventuali impianti di riscaldamento o più spesso condizionamento. L'integrità dei dati possono essere messe a repentaglio da azioni di cracking, errori umani, virus, guasti hardware.

Il piano di disaster recovery deve tenere conto di sia dei possibili livelli di disastro che della criticità dei sistemi e delle applicazioni. Per una corretta applicazione del piano di disaster recovery i sistemi devono essere classificati secondo le seguenti definizioni.

- Critici: nei sistemi critici la funzionalità deve prevedere la sostituzione da parte di strumenti e mezzi di caratteristiche identiche. Le applicazioni critiche non possono essere sostituite con metodi manuali. La tolleranza in caso di interruzione è molto bassa.
- Vitali: nei sistemi vitali la funzionalità può essere sostituita da sistemi manuali per un breve periodo di tempo. Vi è una maggiore tolleranza all'interruzione rispetto a quella prevista per i sistemi critici, e queste funzioni possono essere riattivate entro un breve intervallo di tempo, generalmente stimato in una settimana.
- Delicati: in questi sistemi la funzionalità può essere sostituita da attività manuali per un periodo relativamente lungo. Benché queste funzioni possano essere eseguite manualmente, il loro svolgimento risulta comunque difficoltoso e richiede l'impiego di un numero di persone superiore a quello normalmente previsto in condizioni normali.
- Non critici: in questi sistemi la funzionalità può essere interrotta anche per un lungo periodo di tempo, e viene richiesto un minimo sforzo dopo il ripristino dell'attività.

Le procedure applicative, il software di sistema e i file che sono stati classificati e documentati come critici, devono essere ripristinati prioritariamente. La criticità di applicazioni, software di sistema e dati, deve essere valutata in funzione del periodo dell'anno in cui il disastro può accadere.

Un piano di emergenza deve valutare le strategie di ripristino più opportune attraverso ◀ siti alternativi ▶, metodi di back up, sostituzione dei ruoli e responsabilità del gruppo degli operatori.
Le minacce possibili sono molte e disparate e l'analisi dei relativi rischi deve considerare la loro probabilità e il valore dei dati o dei beni da proteggere. È ovvio che qualsiasi dispositivo e misura di disaster recovery non deve costare più di quanto non valgano i beni stessi da proteggere.

◀ Siti alternativi La prolungata indisponibilità del servizio elaborativo e quindi dei servizi primari, rende necessario l'utilizzo di una strategia di ripristino in sito alternativo. ▶

Un piano di disaster recovery deve considerare i seguenti aspetti:
- costo delle procedure di sicurezza e protezione;
- efficacia di queste misure in riferimento a diversi tipi di rischio;
- analisi dei rischi, delle loro probabilità e livello di pericolo;
- valore dei dati e dei beni da preservare;
- tempi di ripristino della normale funzionalità, o quantomeno della funzionalità minima indispensabile dei sistemi;
- costi necessari per il completo ripristino;
- impatto delle relazioni con l'utenza e con gli stakeholder e metodi per limitarne il danno d'immagine.

◀ Stakeholder Tradotto dall'inglese significa pali di sostegno e indica l'insieme dei soggetti legati a un'azienda o a un'iniziativa economica in genere. Fanno, ad esempio, parte di questo insieme: i clienti, i fornitori, i finanziatori (banche e azionisti), i collaboratori, ma anche gruppi di interesse esterni, come i residenti di aree limitrofe all'azienda o gruppi di interesse locali. ▶

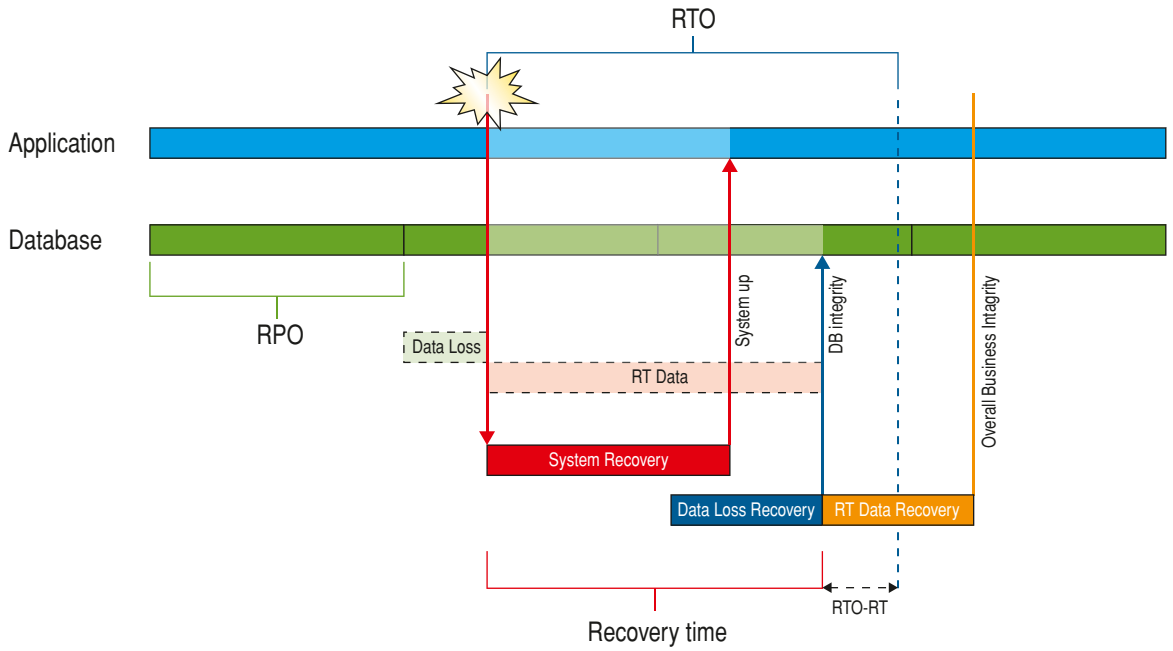
Vediamo un elenco delle principali precauzioni necessarie per prepararci a un disastro e limitarne o prevenirne i danni.
- Backup dei dati. Si tratta di una condizione indispensabile che consente di recuperare facilmente i dati persi. Il supporto su cui viene eseguito il backup deve essere custodito in un luogo ed edificio fisicamente distante, inoltre devono essere eseguiti periodicamente test di ripristino e di verifica dell'integrità dei dati.
- Impianto elettrico a norma, che garantisca sufficiente protezione da fulmini e salti di tensione, con gruppi di continuità che suppliscano a brevi interruzioni di elettricità ed eventualmente generatori per far fronte a prolungati blackout.
- Impianto anti incendio a norma, in grado di individuare ed estinguere automaticamente principi di incendio, senza compromettere la funzionalità dei dispositivi elettronici stessi.
- Linee di backup o di emergenza, in grado di subentrare in caso di guasti di varia natura, tali per cui abbia senso utilizzare per il backup linee di fornitori diversi che si attestino su centrali diverse.
- Altri accorgimenti: tenere le macchine sollevate da terra per limitare i danni da allagamento, fissare le macchine a supporti per evitare cadute accidentali o causate da lievi scosse telluriche, mantenere le macchine in luoghi riparati da umidità o eccessivo calore o sbalzi di temperatura, cablare i cavi in modo che non siano di inciampo.
- Assicurazione sui dispositivi elettronici e sui dati, che copra rischi di varia natura e che copra sia i costi dei danni che quelli dell'eventuale ripristino.

Tecniche di disaster recovery

In caso di disastro i dati considerati importanti, copiati nel sito secondario (Disaster Recovery Site), devono essere resi attivi al più presto e con la minima perdita di dati possibile. I livelli di servizio del sito secondario sono usualmente definiti da due parametri.

1. RTO (Recovery Time Objective) è il tempo necessario per il pieno recupero dell'operatività di un sistema. Rappresenta la durata massima prevista del periodo di inattività (downtime). Il valore di RTO viene definito tenendo presente che se un downtime lungo danneggia la possibilità di fruire del servizio più di uno breve, il danno maggiore deriva dall'inconsapevolezza di quanto possa essere il tempo previsto per il ripristino dei servizi danneggiati.
2. RPO (Recovery Point Objective) indica il tempo massimo che intercorre tra la produzione di un dato e la sua messa in sicurezza, ad esempio attraverso backup e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di un guasto improvviso. Al diminuire dell'RPO richiesto si rendono necessarie politiche di sicurezza sempre

più stringenti e dispendiose, che possono andare dal salvataggio dei dati su supporti ridondanti tolleranti ai guasti fino alla loro pressoché immediata replicazione su un sistema informatico secondario d'emergenza.



Entrambi rappresentano un obiettivo concreto per una soluzione per la continuità e per il ripristino di emergenza. Per migliorarli, occorre aumentare gli investimenti a livello di processi e tecnologie di rete e di archiviazione.

Vediamo le tre tecniche più diffuse per realizzare il recupero dopo eventuali disastri (disaster recovey):

- Replica sincrona. Garantisce che i dati presenti sui due siti sono il più possibile speculari, infatti considera completata una operazione solo se i dati sono stati completamente copiati anche sulla postazione remota. In caso di evento disastroso della sede principale, le operazioni sul sito di Disaster Recovery possono essere riavviate molto rapidamente. La replica sincrona è limitata dalla incapacità dell'applicazione di gestire l'impatto del ritardo di propagazione (vincolo fisico quindi, e non tecnologico) sulle prestazioni. In funzione della sensibilità dell'applicazione e della tecnologia di comunicazione tra i due siti, l'efficacia della copia sincrona inizia a diminuire a una distanza variabile tra i 35 km e i 100 km.
- Replica asincrona. Per far fronte al limite di distanza tra i due siti imposto da tecniche sincrone, si ricorre spesso alla tecnica di copia asincrona. In questo caso il sito che si occuperà della replica può trovarsi anche a distanze notevoli. In questo modo è possibile affrontare anche disastri con ripercussioni su larga scala (come ad esempio forti scosse sismiche) che altrimenti potrebbero coinvolgere entrambi i siti (se questi si trovano nelle vicinanze). Un ulteriore vantaggio della copia asincrona è la possibilità di essere implementata via software non dovendo necessariamente ricorrere a sofisticate e costose tecnologie di storage.
- Tecnica mista. Per garantire la disponibilità dei servizi anche in caso di disastro esteso e al tempo stesso ridurre al minimo la perdita di dati vitali si può ricorrere a una soluzione di tipo misto: effettuare una copia sincrona su un sito intermedio relativamente vicino al primario e una copia asincrona su un sito a grande distanza.

Verifichiamo le conoscenze

1. Completamento

1 Per rendere sicura una rete dobbiamo proteggerla da quattro elementi: ....., ..., ..., ...

2 Si chiama ..... la capacità di un sistema di eseguire normalmente le operazioni malgrado la presenza di errori hardware o software.

3 Per ridurre il rischio di blocchi della rete dobbiamo:
- utilizzare ..... della rete;
- proteggere la rete da ..... che possono compiere atti dolosi o colposi;
- bloccare i tentativi di .....;
- utilizzare le tecniche di .....;
- utilizzare sistemi di controllo ..... degli impianti, dei locali, e delle strutture che li ospitano.

4 Gli attacchi a una rete si possono classificare in due grandi categorie: ....., in cui l'entità non autorizzata accede alle informazioni e le altera in modo da trasmettere informazioni false e ..... che rappresentano i tentativi da parte di terzi di accedere alle informazioni trasmesse durante una comunicazione.

5 Un servizio è sicuro quando garantisce che non possa essere utilizzato per ..... e non si possano ..... le transazioni che avvengono attraverso il servizio stesso.

6 Un frammento sovrapposto può essere usato per tre tipi di attacco:
- attacchi di tipo .....;
- attacchi che prelevano .....;
- attacchi di tipo .....

7 L'attacco ..... consiste nell'inviare un gran numero di richieste a un host con un indirizzo IP sorgente inesistente o non valido.

8 Le ..... sono dovute a imperizia di utenti inesperti o non ben preparati e i danni vanno da danni minimi o irrisori, come ad esempio la cancellazione del profilo, a danni seri come ad esempio quando l'utente tenta di formattare una chiavetta estraibile ed invece formatta un hard disk.

9 Le ..... si hanno quando avviene una manomissione volontaria delle postazioni di lavoro, sono le più gravi in quanto implicano una volontà nella creazione di un danno.

10 Per incrementare la ..... della rete possiamo ..... il flusso di informazioni all'interno della rete e controllare le informazioni che transitano attraverso i ..... e i .....

2. Vero o falso

1 I cracker hanno come obiettivo quello di accedere ai sistemi per puro divertimento, studio o semplicemente per dimostrare di essere in grado di farlo. Solitamente non causano gravi danni al sistema della vittima. V F

2 Gli insiders sono coloro che sono autorizzati all'uso della rete e che cercano di abusarne. V F

3 Un atto o evento che tende a violare la sicurezza delle informazioni trasmesse all'interno della rete, prende il nome di procedura di attacco. V F

4 Nelle reti di grandi dimensioni la funzionalità della rete deve essere garantita dalla fault tolerance. V F

5 La posta elettronica attraverso il protocollo SMTP (Simple Mail Transfer Protocol) è un classico esempio di un servizio sicuro. V F

6 I firewall utilizzano tecniche di packet filtering per difendere la propria rete. V F

7 Le strutture fisiche che ospitano la rete, quindi i locali e gli impianti di climatizzazione, alimentazione e cablaggio devono essere a norma di legge (decreto legislativo 9 aprile 2008 n. 81). V F

8 L'UPS è un sistema di monitoraggio dei server WIndows. V F

Esercitazioni di Laboratorio 4

GESTIRE LE POLICIES CON ACTIVE DIRECTORY

Gli oggetti di Active Directory

Prima di tutto quali sono gli oggetti con i quali A.D. (Active Directory) organizza lo schema logico della rete. Dobbiamo però distinguere tra due tipologie di oggetti:

- oggetti di base (gruppi, utenti e computer);
- oggetti Contenitori (Domini e Unità Organizzative), che contengono al loro interno gli oggetti di base.

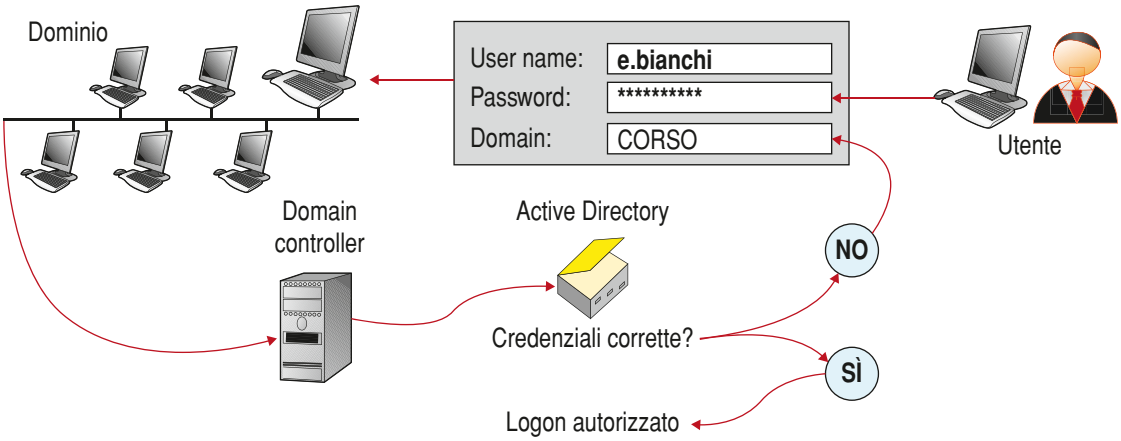
Gli oggetti principali di AD sono i Gruppi e gli Utenti organizzati all'interno di oggetti contenitori come i domini che a loro volta contengono le Unità Organizzative. Ogni utente di un dominio è individuato in modo univoco attraverso uno ◀ user account ▶.

Il processo di Logon, effettuato dall'utente per accedere al dominio, è scandito dalle seguenti fasi:

1. l'utente introduce le proprie credenziali (nome utente, password e scelta del dominio);
2. il DC (Domain Controller) del dominio richiesto verifica la correttezza delle credenziali in Active Directory, autorizzando l'ingresso nel dominio soltanto se Nome Utente e Password sono corrette.

◀ Un utente (User Account) definisce le credenziali di un utente che lo autorizzano ad accedere alla rete attraverso autenticazione (Logon). Le credenziali principali di uno user sono il Nome utente (User Name), la Password e il nome del dominio, che è quello all'interno del quale l'utente stesso dispone dell'account. ▶

Il processo di uscita di un utente da un dominio è quindi denominato Logoff.



La creazione degli user account

La gestione degli account degli utenti può essere fatta in vari modi, secondo la quantità degli stessi e le eventuali procedure definite dall'organizzazione proprietaria della rete. Sulla base delle esigenze di quest'ultima andranno anche determinati gli attributi di cui si vuole tenere traccia in Active Directory. Un'altra decisione importante riguarda la tipologia degli utenti e la loro collocazione. Per quanto riguarda il tipo, gli utenti possono essere locali o di dominio. I primi esistono e possono essere impiegati solo sulla macchina sulla quale vengono definiti, mentre i secondi sono utilizzabili su tutte le macchine che appartengono a un determinato dominio, albero o foresta.
Per quanto riguarda la collocazione, gli utenti e dei gruppi possono essere posizionati sia a livello di dominio sia all'interno delle Organization Unit (OU). La scelta dovrà essere effettuata sulla base delle necessità effettive e della distribuzione delle responsabilità amministrative.

Ciascun user account è individuato da un insieme di ◀ diritti ▶ o privilegi (User rights) e autorizzazioni o permessi (Permission).

◀ I diritti utente definiscono un insieme di autorizzazioni, predefinite in Active Directory, che possono essere assegnate a un account utente in un dominio. Alcuni esempi di user rights sono:
- accesso al computer dalla rete (l'utente può effettuare il logon in un server);
- installa e disinstalla driver periferica (l'utente può caricare e rimuovere dinamicamente i driver delle periferiche);
- arresta il sistema (l'utente può effettuare lo shut down);
- modifica dell'orario di sistema (l'utente dispone dell'autorizzazione per la modifica dell'ora in un server). ▶

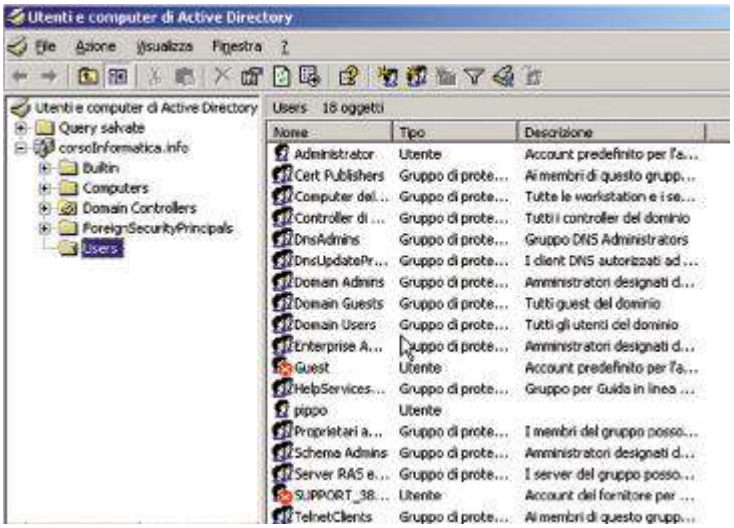
Le autorizzazioni o permessi definiscono i tipi di accesso alle risorse del sistema che è possibile assegnare a un utente e variano da risorsa a risorsa. Alcuni esempi di permessi sono:
- lettura (permesso di lettura per le risorse file e cartelle);
- esecuzione (permesso di eseguire un programma in una cartella);
- stampa (permesso per stampare su una periferica fisica di stampa).

Esistono inoltre degli account utente predefiniti (Built-in) oppure definiti da altri utenti successivamente (User-defined). Gli account utente predefiniti principali sono:
- administrator (l'amministratore dispone di tutte i diritti e i permessi sugli oggetti di Active Directory),
- guest (l'ospite dispone di diritti molto limitati e di nessun permesso predefinito).

Gli utenti User-defined vengono creati appositamente dagli amministratori del dominio, inoltre per ogni account utente creato, gli amministratori si devono preoccupare di assegnare i diritti utente e i permessi necessari per una corretta attività dell'utente nel dominio.
Se gli utenti che dobbiamo creare sono pochi, possiamo eseguire tale operazione direttamente nella console interattiva Utenti e computer di Active Directory, mentre invece se il numero è elevato possiamo usare l'interfaccia ADSI (Active Directory Services Interface).
La procedura che segue mostra come creare un nuovo utente mediante la console interattiva:

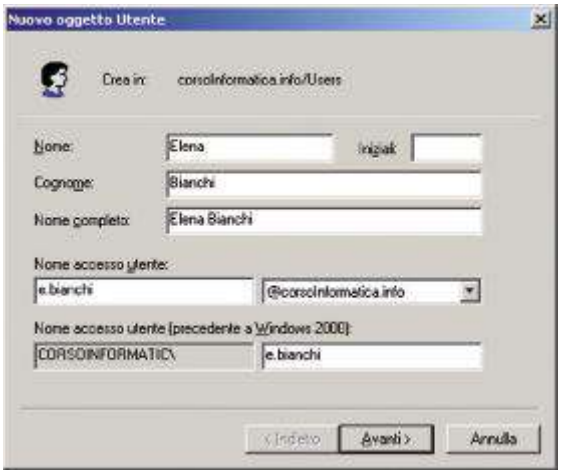
1. Per prima cosa attiviamo la console Utenti e computer di Active Directory, presente nel pulsante Start, quindi Programmi e poi Strumenti di amministrazione:

2 Appare la seguente finestra in cui possiamo notare come nel riquadro di sinistra vi siano gli oggetti logici del sito, mentre nel riquadro di destra si aprano gli elementi presenti in ciascuna categoria di oggetti. In questo caso infatti possiamo avere un elenco di Utenti e gruppi:



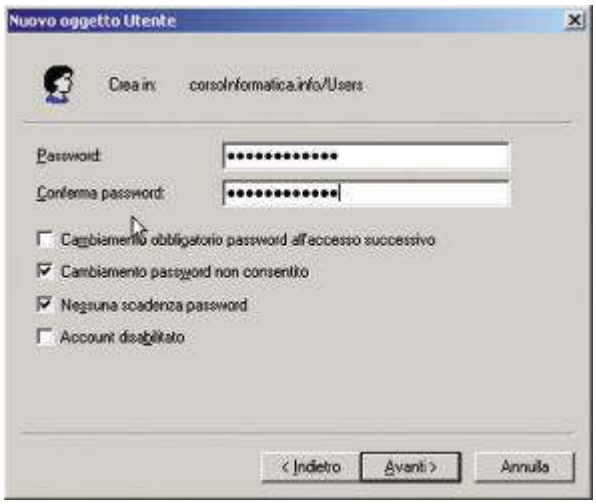
3 Per creare un nuovo utente facciamo clic con il tasto destro su Users e selezioniamo Nuovo e quindi Utente:

4 La finestra che appare ora ci mostra tutto quello che appartiene all'utente, in termini di policies e di permessi a esso assegnati. In questo caso decidiamo di creare l'utente indicato (e.bianchi), ricordando di inserire sempre il Nome accesso utente utile per l'autenticazione (logon) da remoto:



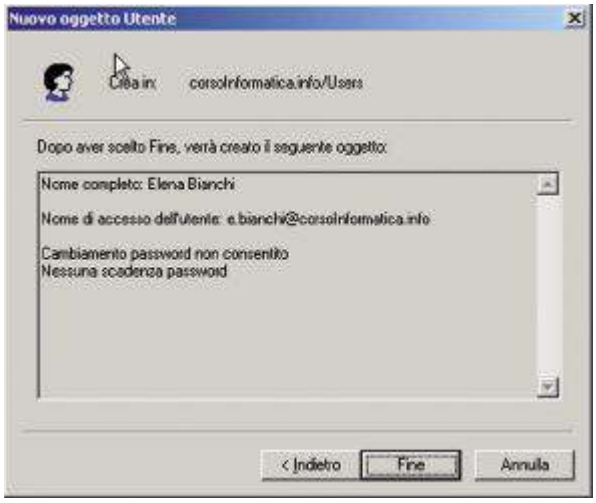
5 Facendo clic su Avanti ci viene richiesta la password, in questo caso ricordiamo che deve contenere almeno un carattere alfabetico maiuscolo, uno minuscolo e un numero ed essere lunga da 8 a 12 caratteri, secondo il criterio di protezione locale di default (Lunghezza minima password).

Per modificare i Criteri di protezione locali, facciamo clic sul pulsante Start, digitiamo secpol.msc nella casella di ricerca e quindi fare clic su secpol. Qualora venisse richiesto, fornire una password amministratore o una conferma. Nel riquadro a sinistra dobbiamo fare doppio clic su Criteri account e quindi fare clic su Criteri password. A questo punto facendo doppio clic sulla voce desiderata dell'elenco Criterio, possiamo modificare l'impostazione.



Se la password non soddisfa i criteri impostati nei criteri di protezione locale, non verrà accettata e sarà necessario inserirne un'altra valida.

6 A questo punto ci viene mostrata una finestra che riepiloga le informazioni dell'utente appena creato. Facciamo clic su Fine:



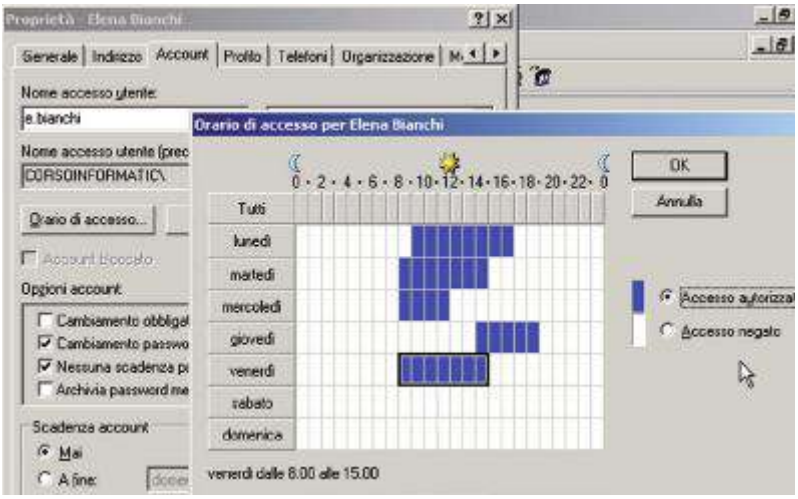
7 L'utente è stato creato e appare nell'elenco Users.

Modificare le impostazioni degli account utenti

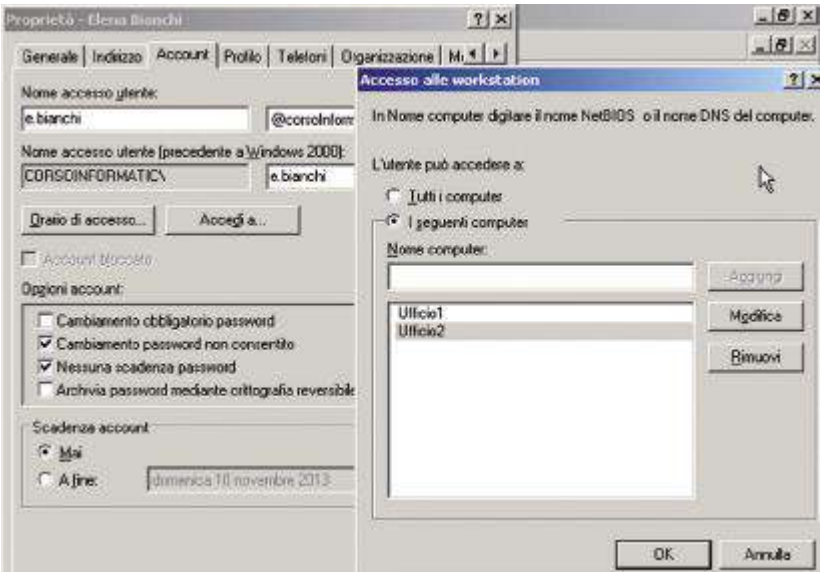
Vediamo come assegnare all'utente un account e le relative autorizzazioni di accesso alle risorse.

1. Facendo sull'utente che vogliamo gestire con il tasto destro del mouse e scegliamo Proprietà:

2. Appare una finestra con diverse schede: Generale, Indirizzo, Account, Profilo, Telefoni, Organizzazione ecc. Posizioniamoci sulla scheda Account per modificare le autorizzazioni di accesso al server di dominio. Per fare questo facciamo clic su Orario di accesso... e selezioniamo alcuni orari, come mostrato dalla seguente immagine:



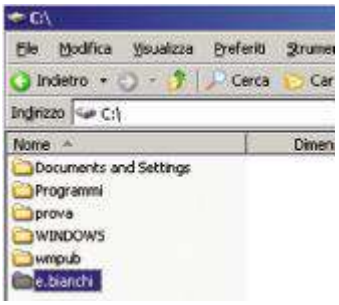
3. Possiamo anche limitare l'accesso all'utente da determinati computer della rete. Ad esempio in questo caso l'accesso è limitato ai due soli computer (Ufficio1 e Ufficio2):



Creare una Home directory per l'utente

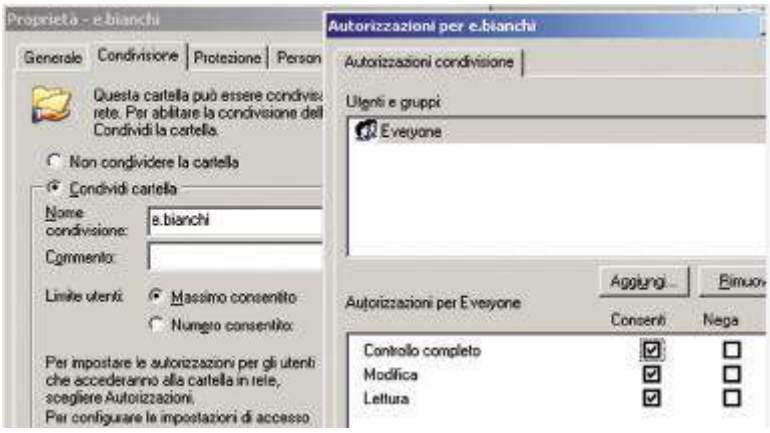
In questo caso vogliamo creare una Home directory per un utente. Per fare questo seguiamo la seguente procedura:

1. Per prima cosa dobbiamo creare la directory che fungerà da Home directory per l'utente e.bianchi che abbiamo creato in precedenza. Andiamo nella root del disco rigido e in questo caso chiamiamo la directory con il nome dell'utente:



2. Adesso dobbiamo condividerla. Per fare questo facciamo clic con il tasto destro e selezioniamo la voce Proprietà:

3. Andiamo nella scheda Condivisione e facciamo clic sul pulsante Autorizzazioni. Associamo al gruppo Everyone il Controllo completo sulla cartella in modo tale da regolare poi i permessi per il singolo utente, ricordando che vige sempre l'autorizzazione più restrittiva:



4. Adesso dobbiamo assegnare i permessi NTFS all'utente e.bianchi in modo che possa utilizzare la cartella dalla rete. Per fare questo ci posizioniamo nella scheda Permessi. Come possiamo notare nell'elenco dei gruppi e utenti non appare l'utente che ci interessa, dobbiamo fare clic su Aggiungi per aggiungerlo:

5 Nella finestra che compare scriviamo il nome dell'utente da aggiungere e facciamo clic su Controlla nomi per verificare se il nome è corretto, il sistema provvederà a cercarlo nel database di A.D. e riscriverlo correttamente secondo la notazione di sistema. Se appare correttamente facciamo clic su OK per confermare:

6 Come possiamo notare il nostro utente è stato aggiunto all'elenco dei beneficiari di questa cartella. Facciamo clic sul permesso Modifica e per consentirne l'accesso e quindi OK per confermare:

7 Come possiamo notare la cartella è adesso condivisa, possiamo notare la mano sotto la cartella:

8 Per assegnare la cartella creata come ◀ Home directory ▶ per l'utente dobbiamo prima di tutto conoscerne l'indirizzo, in questo caso rappresentato dalla radice del disco.

◀ Una home directory è una cartella (directory) del sistema operativo destinata a contenere i file personali di uno specifico utente del sistema, assegnata all'utente dall'amministratore di sistema o dal sistema operativo stesso. È in genere presente nel Server di dominio sul quale è stato installato Active Directory. ▶

9 Selezioniamo l'utente desiderato nella console di Utenti e Computer di Active directory e facciamo clic con il pulsante destro, quindi Proprietà:

10 Apriamo la scheda Profilo e aggiungiamo il percorso della cartella creata nel passo precedente nella casella Connetti:, secondo il formato seguente:

◀ Il formato UNC definisce i percorsi delle directory o dei server. Per i server dobbiamo ricordare che Windows li interpreta seguiti dal doppio backslash (\\). Quindi il server di nome DC si chiamerà secondo il formato UNC: \\DC. ▶

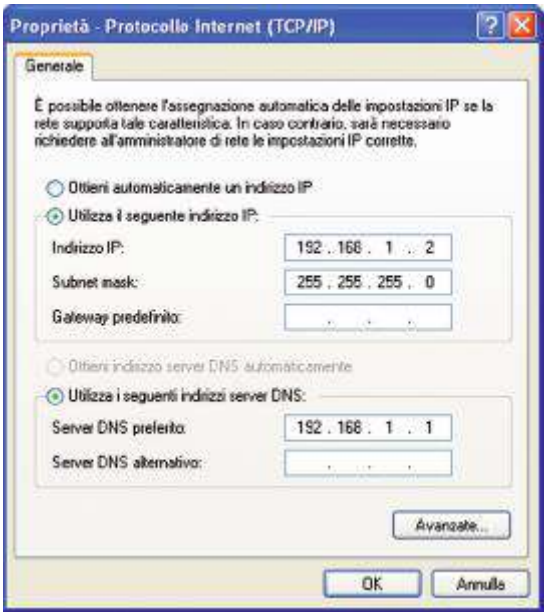
\\nome del server in formato ◀ UNC ▶ (Universal Naming Convention) \ seguito dalla directory.

11 A questo punto facciamo clicl su OK, la Home directory è stata creata. Per verificarne l'utilizzo dobbiamo tuttavia ancora collegare un computer client al server di dominio, che vedremo nel prossimo paragrafo.

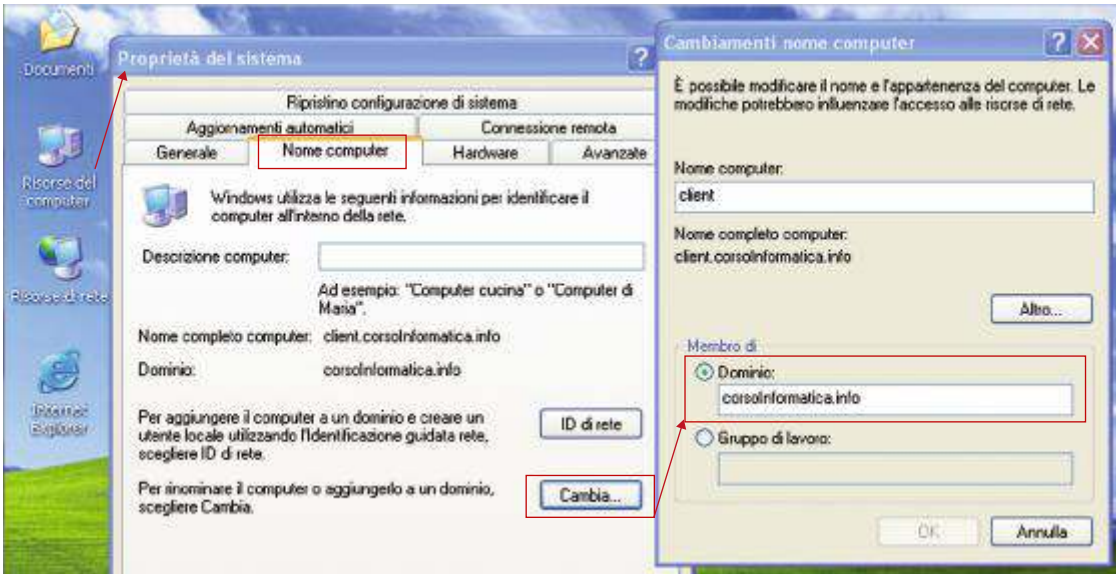
L'accesso al server di dominio dal client

La seguente procedura illustra come assegnare a un host del dominio l'accesso al dominio stesso.

1. Per prima cosa dobbiamo accedere al computer con le credenziali di amministratore locale. Quando abbiamo acceso il nostro computer, dobbiamo prima di tutto configurare la scheda di rete per collegarci alla LAN del sito di dominio. Per fare questo dovremo semplicemente assegnare l'indirizzo IP, secondo la modalità statica o dinamica o dinamica progettata prioritariamente, quindi indicare l'indirizzo del DNS che deve coincidere con il DNS Server del dominio:

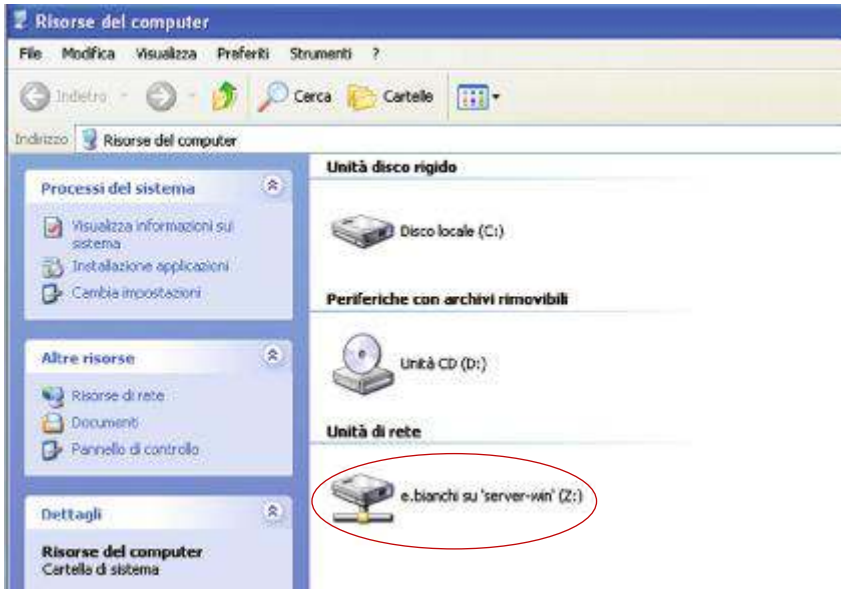


2. La seconda fase è quella di assegnare il dominio di appartenenza, dopo aver fatto clic con tasto destro sull'icona di Risorse del computer, selezioniamo la scheda Nome computer, quindi scriviamo il nome del dominio nella casella Membro di Dominio:, in questo caso corsoInformatica.local:

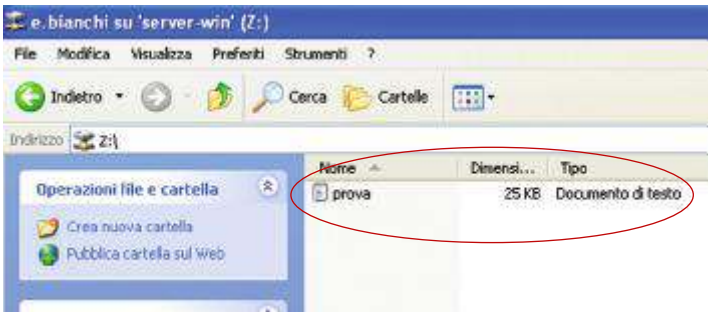


3 Adesso possiamo riavviare la macchina. All'accesso successivo inseriamo le credenziali dell'utente di dominio (in questo caso e.bianchi). Come possiamo notare appare il dominio nella casella combinata posta in basso nella finestra di Logon:

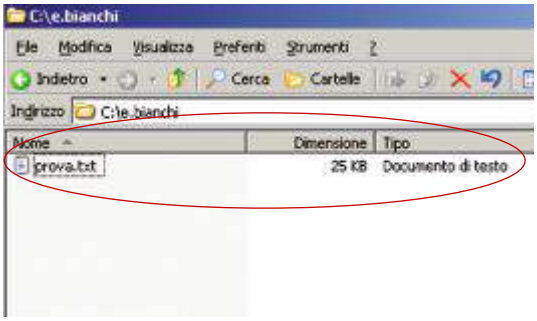
4 Se apriamo le Risorse del computer possiamo notare che appare automaticamente la Home directory dell'utente:



5 Adesso proviamo a creare un file (prova.txt) all'interno della Home directory del nostro client di dominio, si tratta di una verifica che il sistemi funzioni effettivamente:



6 Se il sistema funziona correttamente dovremo trovare, nella corrispondente directory presente sul server di dominio, lo stesso file creato dal client:



7 Adesso proviamo, sempre dal computer client, ad aprire una directory qualunque sul server, come possiamo notare il messaggio ci informa che non possediamo le autorizzazioni necessarie per aprirla:

Prova adesso!

- Utilizzare le policies di Windows Server

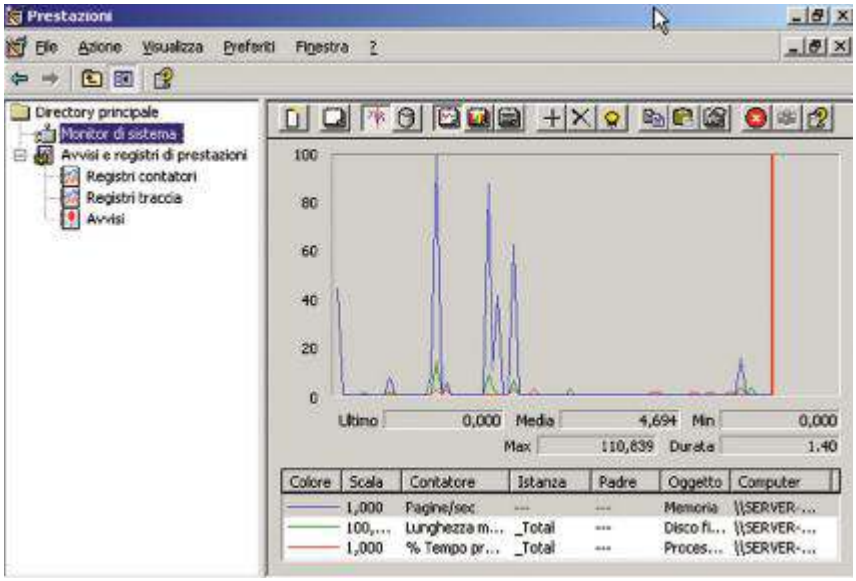
1 Crea un utente per ogni tuo compagno di classe e assegna a esso una diversa home directory.
2 Verifica l'accesso dal client, oltre a verificare che possa accedervi solo l'utente corretto.

Esercitazioni di Laboratorio 5

IL MONITORAGGIO DI WINDOWS SERVER

Il monitoraggio

L'amministrazione del server deve garantire innanzi tutto la sicurezza ma anche l'affidabilità del sistema rete a dominio o comunque rete in senso più ampio. Il monitoraggio garantisce l'efficienza di una rete client server migliorandone le prestazioni, cioè il tempo con cui un host completa le attività di sistema e le applicazioni.
Le prestazioni di un sistema possono essere danneggiate da diversi fenomeni, prima di tutto la lentezza dei dischi o del relativo accesso ai dati in essi contenuti, l'insufficiente quantità di memoria disponibile per i processi in esecuzione, oppure ancora la velocità effettiva delle interfacce di rete o dei cavi di collegamento.
Il principale strumento di analisi delle prestazioni su Windows Server è la console Prestazioni (Performance), che contiene gli strumenti Monitor di Sistema (System Monitor) e Avvisi e registri di prestazioni (Performance Logs).

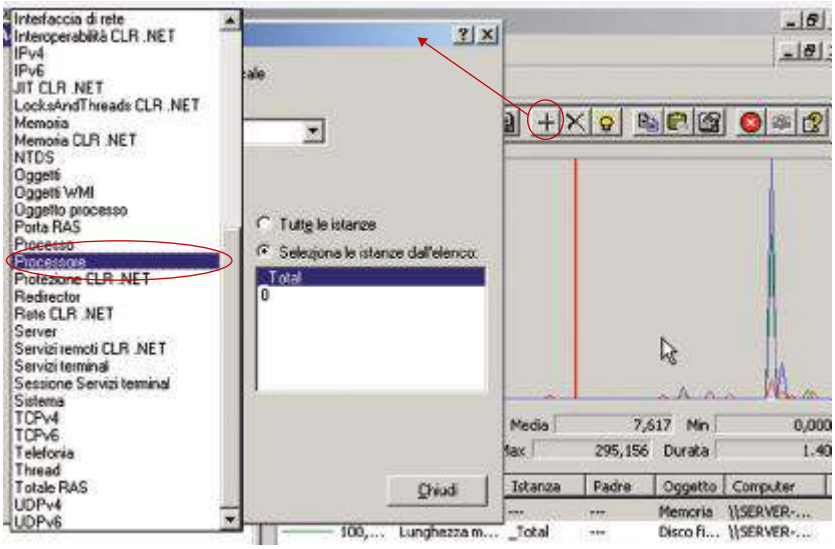


Monitor di sistema

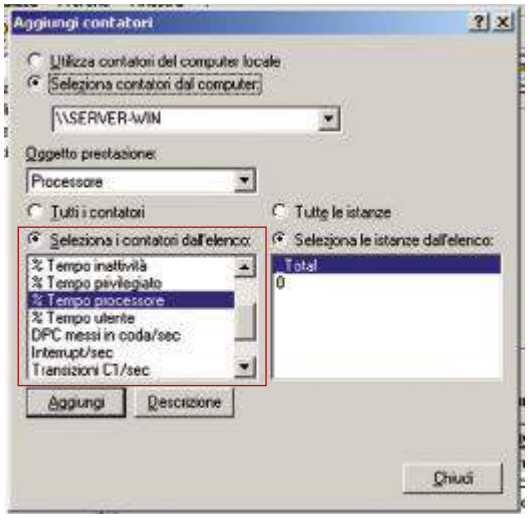
Attraverso il Monitor di sistema possiamo tenere sotto controllo in tempo reale i servizi di sistema e le risorse hardware utilizzate. Possiamo in tal modo controllare sia il sistema dove si esegue lo

strumento sia un server remoto. Il monitor visualizza i dati relativi a dei contatori liberamente selezionabili, in base alle nostre esigenze. Al nostro monitor possiamo aggiungere:

- oggetti prestazione che in genere corrispondono ai principali componenti hardware, ad esempio memoria, Thread, processore, interfaccia di rete ecc. Per attivarlo devi cliccare sul pulsante "+" e selezionare l'oggetto dall'elenco a tendina della voce oggetti prestazione:



- contatori, associati a ogni oggetto prestazione, rappresentano aspetti specifici di un sistema o di un servizio. Ad esempio, il contatore Pagine/sec associato all'oggetto Memoria tiene traccia dell'indice di paging della memoria.



Per monitorare le prestazioni di un computer diverso da quello in cui verrà eseguito il servizio Avvisi e registri di prestazioni, dobbiamo fare clic con il tasto destro sulla finestra del monitor, aggiungere un contatore, fare clic su Selezionare gli oggetti contatore dal computer e specificare il nome del computer che si desidera controllare in formato UNC (Universal Naming Convention), come ad esempio \\computer2.

Registri contatori (counters logs)

Per memorizzare i dati relativi alle prestazioni del sistema possiamo utilizzare lo strumento Avvisi e registri di prestazioni; in questo modo possiamo creare un registro contatore, personalizzabile con l'aggiunta di oggetti e relativi contatori. La seguente procedura illustra come creare un registro contatore:

1. Apri Start, quindi Pannello di controllo, Strumenti di amministrazione e seleziona Prestazioni.
2. Espandi la voce Avvisi e registri di prestazioni e posizionati su Registri contatori. Nel riquadro di destra possiamo così vedere l'elenco dei registri contatori esistenti, colorati di verde se il registro è in esecuzione, di rosso se in stato di arresto.

3. Seleziona Nuove impostazioni registro, facendo clic con il tasto destro del mouse sulla voce registri contatori e scrivi il nome del nuovo registro contatore da creare confermando poi con OK.
4. Appare a quel punto la scheda Generale in cui devi fare clic su Aggiungi oggetti per selezionare gli oggetti prestazioni da aggiungere, oppure fare clic su Aggiungi contatori per selezionare i contatori da registrare. Possono anche essere selezionati oggetti e contatori relativi a un sistema remoto.

> Se vogliamo modificare le informazioni predefinite sulla pianificazione e sui file, dobbiamo apportare le modifiche nelle schede File registro e Pianificazione.

5. Dopo aver creato un registro contatore, un registro traccia o un avviso, è possibile salvarlo facendo clic su di esso con il pulsante destro del mouse nel riquadro dei dettagli e quindi scegliere Salva impostazioni con nome. Sarà quindi possibile specificare un file .htm in cui salvare le impostazioni. Per riutilizzare le impostazioni salvate per un nuovo registro o avviso, fare clic con il pulsante destro del mouse sul riquadro dei dettagli, quindi scegliere Nuove impostazioni registro da o Impostazioni nuovo avviso da. Esiste anche la possibilità di aprire il file HTML in Internet Explorer per visualizzare un grafico di Monitor di sistema.

Zoom su...

SALVARE UN REGISTRO CONTATORE

Un registro contatore può essere memorizzato sotto diverse forme.

- File di testo (csv): questa opzione definisce un file registro delimitato da virgole con estensione .csv. Utilizzare questo formato, ad esempio, per esportare i dati del registro in un foglio di calcolo.
- File di testo (delimitato da tabulazioni): definisce un file registro delimitato da tabulazioni con estensione .tsv.
- File binario: Questa opzione definisce un file registro sequenziale in formato binario con estensione .blg. Utilizzare questo formato per registrare istanze di dati intermittenti, ovvero che si interrompono e riprendono dopo che è iniziata l'esecuzione del registro.
- File circolare binario: questa opzione definisce un file registro circolare in formato binario con estensione .blg. Utilizzare questo formato per registrare continuamente i dati nello stesso file registro, sovrascrivendo i record precedenti con i nuovi dati quando vengono raggiunte le dimensioni massime del file.
- Database SQL: questa opzione consente di definire il nome di un database SQL esistente e un set di registri all'interno del database in cui leggere o scrivere i dati sulle prestazioni. Utilizzare questo formato di file se si desidera raccogliere i dati sulle prestazioni a livello di organizzazione piuttosto che a livello di server.
- Vediamo ora nel dettaglio quali sono i contatori e i valori da monitorare per le principali componenti del nostro sistema.

Monitoraggio della memoria

Quando il sistema è lento dobbiamo verificare la memoria RAM, se infatti la capacità della RAM installata è insufficiente, le applicazioni e i servizi in esecuzione nel server risulteranno assai lente, secondo la tipica rappresentazione a collo di bottiglia (bottleneck). Il ◀ paging ▶ eccessivo è il primo indicatore di un quantitativo insufficiente di RAM.

◀ Il paging è un processo con cui blocchi di codice vengono spostati dalla memoria RAM fisica alla memoria virtuale su disco rigido, ed è rappresentata da un particolare file detto di appunto di paging o di swap. ▶

La memoria virtuale viene sempre utilizzata dal sistema anche quando la memoria fisica richiesta da tutti i processi non supera la quantità di RAM fisica effettivamente installata nel sistema. Tuttavia quando questa richiesta si avvicina al valore limite della RAM disponibile, il sistema operativo sposterà con maggiore frequenza blocchi di dati dalla RAM al file di paging, liberando memoria fisica per altri utilizzi, ma facendo uso eccessivo di operazioni di lettura scrittura su disco, a discapito di tutte le altre operazioni in esecuzione sul sistema.

Vediamo quali sono i principali contatori da utilizzare per monitorare la memoria.

- Pagine/sec: visualizza la frequenza con la quale le pagine vengono lette dal disco o scritte sul disco per risolvere gli errori di pagina gravi. Si verificano errori di pagina quando il sistema cerca nella memoria RAM fisica pagine che non sono più disponibili, in quanto spostate nel file di paging. Il suo valore medio, misurato su un periodo campione, dovrebbe essere in genere <5.
- Byte disponibili: indica la quantità totale di memoria fisica disponibile. Il contatore presenta normalmente valori bassi in quanto Windows Disk Cache Manager usa memoria extra per la cache di sistema e restituisce memoria quando i processi ne fanno richiesta. Tuttavia bassi valori di Byte disponibili, <=5% della memoria fisica totale, possono indicare un'insufficienza generale di memoria oppure il mancato rilascio di memoria da parte di un programma.

- Byte vincolati: indica il totale di memoria virtuale allocata dai processi. Se questo valore è superiore alla memoria RAM fisica installata è necessario aggiungere altra memoria al sistema. Un valore elevato di questo contatore rispetto alla RAM fisica installata causa l'eccessivo utilizzo del file di paging, con rallentamento dell'intero sistema.
- Byte del pool non di paging: indica il numero di pagine che non possono essere spostate nella memoria virtuale e che quindi devono rimanere nello spazio della memoria fisica. Se questo valore subisce un incremento senza un corrispondente aumento delle attività nel server, l'incremento stesso potrebbe essere dovuto a un processo con memory leak, che significa falla nella memoria, cioè un consumo eccessivo di RAM dovuto alla mancata deallocazione dalla memoria di variabili non più utilizzati nel processo. Questo valore dovrebbe mantenersi abbastanza costante.

Paging e uso del disco

Un'elevata attività di paging comporta di conseguenza un relativo utilizzo del disco, tuttavia non dobbiamo confondere i problemi di memoria insufficiente, con i colli di bottiglia del disco. Se verifichiamo che l'eccessivo paging non dipende dall'insufficiente memoria RAM installata dobbiamo monitorare il disco attraverso i suoi oggetti e contatori, che possono essere così sintetizzati:

Oggetto	Contatore
Disco logico	% Tempo disco
Disco fisico	Lunghezza media coda del disco

Se riscontriamo una bassa frequenza di operazioni di lettura delle pagine tramite il monitor Memoria Pagine/sec. ma contemporaneamente alti valori di %Tempo disco e Lunghezza media coda del disco, i rallentamenti del sistema potrebbero essere causati da un collo di bottiglia del disco. Se, invece, all'aumento della lunghezza della coda corrisponde un aumento di lettura delle pagine su disco, il problema dipende da un'insufficienza di memoria.

Monitoraggio dei dischi

Per monitorare i dischi e le attività relative possiamo usare i seguenti contatori:

- Disco fisico: % Tempo disco: indica la percentuale di tempo dedicata dal disco ad attività di lettura o scrittura. Il valore medio non dovrebbe mai essere superiore al 90%
- Disco fisico: Lunghezza media coda del disco: indica il numero di richieste che provengono dal sistema e che sono state messe in una coda di attesa. Il valore non dovrebbe mai superare il valore dato dal numero di cilindri più 2. Al contrario, i dispositivi RAID utilizzano più cilindri, dati dal numero di hard disk che compongono il RAID. Un dispositivo RAID hardware viene visualizzato come un disco fisico in Monitor di sistema.
- Media Byte/Trasf. Disco: indica il valore medio di byte trasferiti nel disco durante le operazioni di lettura e scrittura. Più efficiente sarà la sezione dischi del nostro sistema, maggiore sarà il valore visualizzato.
- Byte da/a disco /sec.: indica i byte trasferiti nel disco durante le operazioni di lettura e scrittura. Più efficiente sarà la sezione dischi del nostro sistema, maggiore sarà il valore visualizzato.
- Disco logico: % spazio disponibile: indica la quantità di spazio disponibile su un disco logico (unità C, D ecc.)

> L'assenza di un quantitativo adeguato di memoria fisica RAM porta a un'elevata attività di paging, con un utilizzo considerevole del disco. Pertanto i problemi di memoria insufficiente che provocano il paging possono essere confusi con una lentezza del disco. Se il paging non sembra imputabile ai dischi, verificare il contatore Pagine/sec relativo all'utilizzo della memoria, il cui valore non dovrebbe essere superiore a 5.

Monitoraggio del processore

Il monitoraggio del processore può essere eseguito sia con gli strumenti della console (Prestazioni), sia con il Task Manager. Su Task Manager, il primo parametro da verificare è la percentuale di tempo in cui il processore è impegnato nelle operazioni di calcolo, visualizzabile alla voce Utilizzo CPU. Sulla console Prestazioni, i contatori da utilizzare per determinare se il processore è un collo di bottiglia per il sistema sono i seguenti.

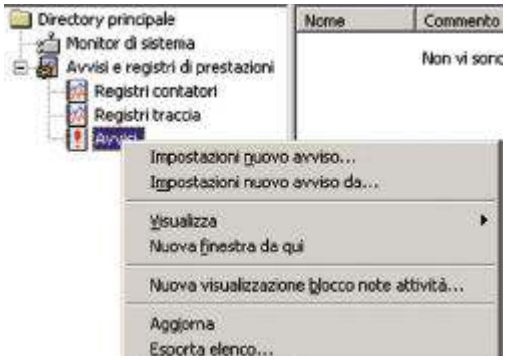
- % Tempo processore: indica la percentuale di tempo che il processore impiega per eseguire i processi eccetto il processo idle, sottraendo il tempo dei processi idle dal 100%. In sostanza rappresenta il tempo che il processore impiega per normali processi, percentuale che dovrebbe mantenere un valore medio inferiore all'85%.
- Sistema/lunghezza coda processore: indica il numero di richieste al processore che sono rimaste in coda, quindi rappresenta i processi pronti per l'esecuzione ma in attesa che il processore si liberi. Il valore accettabile solitamente è inferiore a 2.
- Code di lavoro del server/lunghezza coda: indica la lunghezza corrente della coda di lavoro del server relativa al processore selezionato. Il valore accettabile dovrebbe essere inferiore a 4.
- Interrupt/sec: indica il numero di interrupt generati dai processi come ad esempio i controller degli hard disk e le interfacce di rete. Il valore superiore a 1000 indica certamente dei problemi di tipo hardware.

Monitoraggio della rete

Il controllo del funzionamento corretto del flusso dei dati in una rete consiste nel monitorare l'utilizzo delle risorse del server e nel misurarne il traffico complessivo. I principali contatori che verificano le attività di rete sono:

- % Utilizzo rete: è presente nel Task Manager di Windows: indica la percentuale di banda di rete in uso per l'interfaccia di rete locale. Il suo valore dovrebbe stare al di sotto del 30%.
- Interfaccia di rete: Byte inviati/sec.: indica il numero di byte inviati tramite l'interfaccia di rete.
- Interfaccia di rete: Byte totali/sec.: indica il totale dei byte inviati e ricevuti tramite l'interfaccia di rete. Il valore dovrebbe essere elevato, in tal caso si è in presenza di un alto numero di trasmissioni con successo.
- Server / Byte ricevuti/sec.: è un valore da confrontare con la larghezza di banda totale a disposizione per l'interfaccia di rete. Il valore dovrebbe essere inferiore al 50% della capacità.

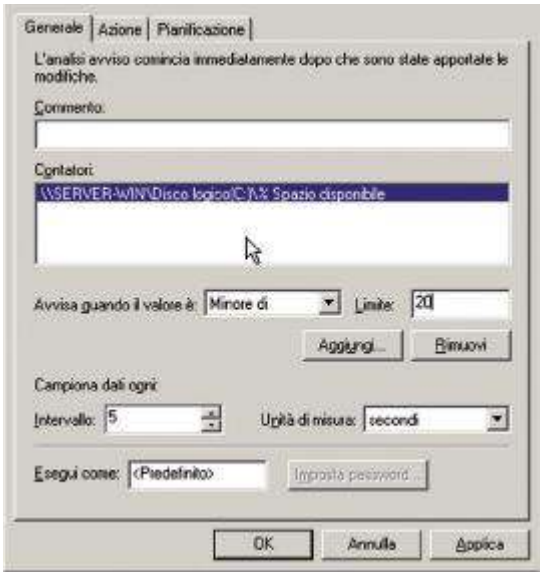
Windows Server consente di memorizzare messaggi nel log eventi, eseguire applicazioni particolari oppure inviare messaggi in rete quando il valore di un contatore è al di fuori della soglia di controllo impostata dall'amministratore. Questa operazione può essere effettuata mediante lo strumento Avvisi, presente in Avvisi e registri di prestazioni all'interno della console Prestazioni di Windows. Possiamo ad esempio usare un avviso per monitorare alcune prestazioni del sistema. Gli avvisi possono essere gestiti anche dalla postazione client dell'amministratore, attraverso la console Prestazioni, quindi Avvisi, e infine Impostazioni nuovo avviso.



Facendo clic su Aggiungi nella scheda Generale delle Proprietà della scheda di segnalazione possiamo impostare contemporaneamente più avvisi di monitor che riguardano più server in rete. Per esempio volendo ricevere un avviso che ci informa sullo spazio libero nell'unità disco di un server, nella finestra di dialogo Aggiungi contatori è necessario selezionare o digitare il nome di un server,

selezionare l'oggetto Disco Logico, selezionare il contatore %Spazio disponibile, selezionare il volume appropriato e fare clic su Aggiungi:

In questo modo possiamo ad esempio aggiungere un contatore per ogni volume desiderato su ogni server. Dopo aver cliccato su chiudi, nella scheda Generale è necessario selezionare il contatore per il quale impostare la soglia di avvertimento, impostando ad esempio Minore di 10 per ricevere un avviso quando lo spazio libero nell'unità è inferiore al 20%.



Se lasciamo attivato il segno di spunta sulla voce Registra una voce del registro... l'evento verrà catalogato all'interno del registro eventi applicazione presente nella macchina in cui sono eseguiti gli eventi monitor.

Possiamo anche impostare l'esecuzione di un'applicazione o l'invio di un messaggio attraverso la rete; inoltre, nella scheda Pianificazione, possiamo specificare uno schema in base al quale verranno avviate le analisi. Quando una segnalazione viene inviata, oltre all'invio del messaggio in rete verrà memorizzato nel log eventi il nome del contatore, oltre al computer e alla lettera dell'unità di volume e al relativo superamento della soglia specificata.

Prova adesso!

• Utilizzare i monitor di sistema

Verifica l'utilizzo delle seguenti risorse:
- scheda rete;
- processore;
- memoria;
- disco.

Impostando almeno due eventi e contatori, facendo apparire un messaggio in caso di superamento delle soglie. Per quanto riguarda le soglie utilizza quelle consigliate in questa lezione.

Esercitazioni di Laboratorio 6

FILE SERVER E PROTEZIONE NTFS

In questa lezione di laboratorio vedremo come realizzare un file server con Windows Server, partendo dal ripasso dei concetti che sono alla base delle policies di NTFS.

Permessi e condivisioni

Mentre i permessi di condivisione valgono solo nel caso di accessi via rete e si possono specificare solo per cartelle, i permessi NTFS valgono localmente e si possono specificare per le cartelle ma anche per il singolo file.
Possiamo anche specificare i permessi NTFS sia per il singolo utente che per gruppi di utenti e anche per loro è utilizzabile la strategia AGDLP vista nelle lezioni precedenti. Come abbiamo visto nelle lezioni precedenti, le access control list (ACL) contengono la lista degli utenti, dei gruppi e dei computer che hanno accesso alle risorse e il tipo di accesso concesso.
Per poter accedere a una risorsa la ACL di un utente deve contenere almeno una access control entry (ACE) relativa al particolare utente o a uno dei gruppi cui appartiene.

Zoom su...

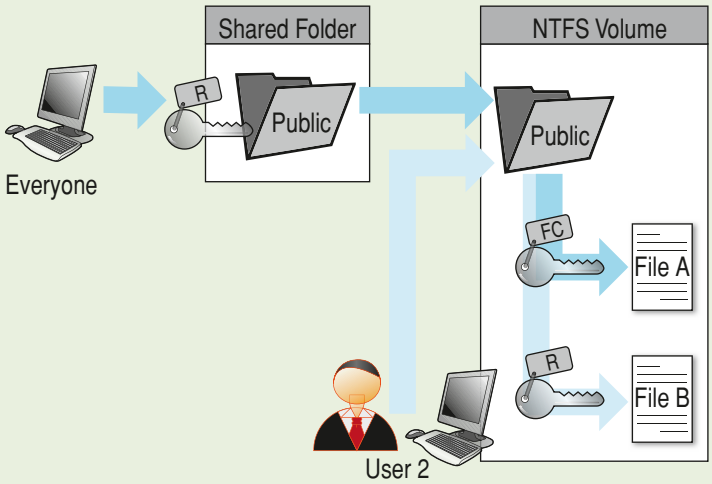
Riassumiamo i permessi NTFS associabili a cartelle:
- Lettura. Visualizzare file e cartelle e i relativi attributi, proprietari e permessi.
- Scrittura. Creare nella cartella nuove cartelle e file, modificarne gli attributi e vederne proprietari e permessi.
- Visualizzazione contenuto cartella. Visualizzare i nomi dei file e delle cartelle contenute nella cartella.
- Lettura ed esecuzione. Navigare attraverso le cartelle, lanciare eseguibili oltre ai permessi di Lettura e Visualizzazione contenuto cartella.
- Modifica. Eliminare la cartella oltre ai permessi Scrittura e Lettura ed esecuzione.
- Controllo completo. L'unione di tutti i permessi precedenti.

I permessi NTFS associabili ai file hanno precedenza rispetto a quelli che il *file* eredita dalla cartella che lo contiene. Riassumiamo i permessi NTFS associabili ai file:
- Lettura. Leggere il file e visualizzarne gli attributi, oltre a vederne il proprietario e i permessi.
- Scrittura. Modificare il file, gli attributi e vederne il proprietario e i permessi.
- Lettura ed esecuzione. Eseguire applicazioni oltre ai permessi di Lettura.

- Modifica. Modificare ed eliminare il file oltre ai permessi di Scrittura e Lettura ed esecuzione.
- Controllo completo. L'unione di tutti i permessi precedenti.

Nel caso di permessi contradditori, come ad esempio se consentiamo l'accesso per un utente al quale era stato negato l'accesso del gruppo a cui appartiene, il permesso più restrittivo ha sempre la meglio. In sintesi vediamo quali sono le principali linea guida nell'assegnazione di permessi NTFS:
- Rimuovere il permesso Controllo completo dal gruppo Everyone.
- Assegnare il permesso Controllo completo al gruppo Administrators.
- Assegnare al Creator Owner Controllo completo delle sue cartelle dati.
- Educare gli Users nell'assegnare i permessi NTFS ai propri *file*.

Per la Home directory:
- Creare una cartella centrale denominata Users.
- Condividere la cartella Users.
- Rimuovere il permesso Controllo completo dal gruppo Everyone e assegnarlo al gruppo Users.
- Usare la variabile d'ambiente %Username% per creare le home directory.

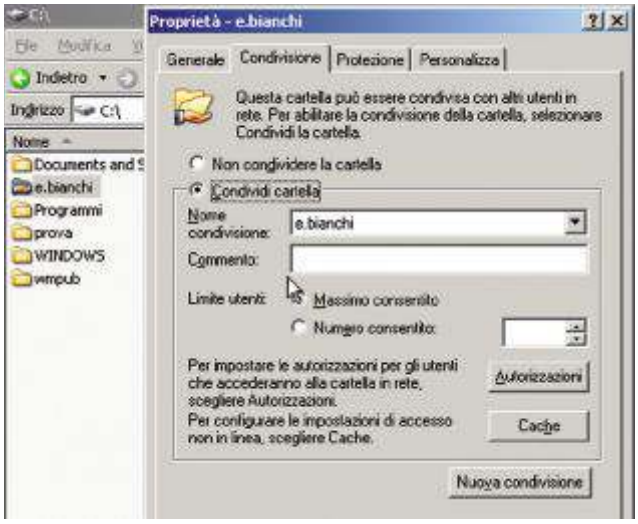


Per poter assegnare i permessi NTFS a un qualsiasi oggetto si devono rispettare alcuni requisiti fondamentali, quali:
- esserne il proprietario;
- godere dell'insieme di permessi Controllo completo o almeno del permesso Cambia autorizzazioni o Diventa proprietario.

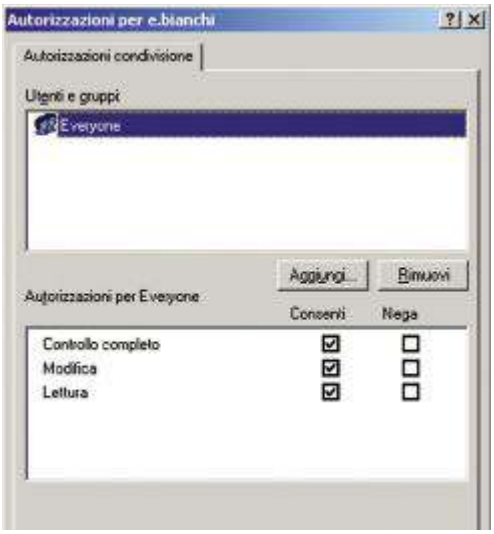
Condivisione di file in Windows

Le Cartelle Condivise sono uno strumento che consente agli utenti l'accesso dalla rete. A motivo di questo è necessario garantire delle policies che determinino l'accesso a tali cartelle. Per poter condividere una cartella dobbiamo appartenere a uno dei gruppi che possiedono il diritto di condivisione cartelle nel *computer* in cui la cartella risiede. Quando condividiamo una cartella dobbiamo:
- assegnare a essa il nome di condivisione;
- limitare eventualmente il numero di utenti che si possono connettere contemporaneamente a tale condivisione;
- assegnare i permessi a gruppi di utenti o singoli utenti;
- possiamo anche condividere la stessa cartella più volte.

Per condividere una cartella in un Windows Server dobbiamo selezionare la cartella, quindi dopo aver fatto clic con il tasto destro su di essa selezioniamo la scheda Condivisione che specifica le seguenti opzioni:



- Condividi questa cartella. Selezionare tale opzione per condividere la cartella.
- Nome condivisione. Specifica il nome che verrà assegnato alla condivisione e che verrà utilizzato dall'utente e dalle applicazioni ogni qualvolta intendano accedere a essa.
- Commento. Descrizione opzionale, che ha lo scopo di identificare il contenuto e lo scopo della condivisione.
- Limite utenti. Specifica il numero massimo di accessi concorrenti permessi a questa condivisione. Non è obbligatorio poiché il valore di default è in genere pari al numero di licenze acquistate.
- Autorizzazioni. Con questo pulsante viene mostrata la finestra che permette di assegnare permessi di accesso alla cartella condivisa a utenti o a gruppi:



A ciascun utente, gruppo o computer può essere garantito o negato il permesso di accedere alla condivisione.

> I permessi di condivisione non proteggono la risorsa da accessi locali e valgono per l'intera cartella, quindi anche a tutto il suo contenuto.

Le autorizzazioni di condivisione sono le seguenti:

- Controllo completo. Possiamo modificare i file contenuti, oltre al fatto che diventiamo proprietari della cartella.
- Modifica. Oltre a tutto ciò che è garantito da Lettura possiamo creare cartelle, aggiungere *file*, modificare *file*, modificare gli attributi, eliminare *file* e cartelle.
- Lettura. Possiamo visualizzare i nomi delle cartelle, dei *file*, dei i dati contenuti nei *file*, gli attributi ed eseguire programmi.

I permessi di condivisione sono cumulativi: quando un utente accede a una condivisione e in questa condivisione sono stati specificati sia permessi per l'utente che per alcuni o tutti i gruppi cui l'utente appartiene, allora il permesso risultante per quell'utente è la somma di tutti i permessi. Tale regola ammette una sola eccezione: se solo uno dei permessi è Nega allora tutti gli altri permessi vengono sovrascritti e il permesso risultante sarà un Nega.

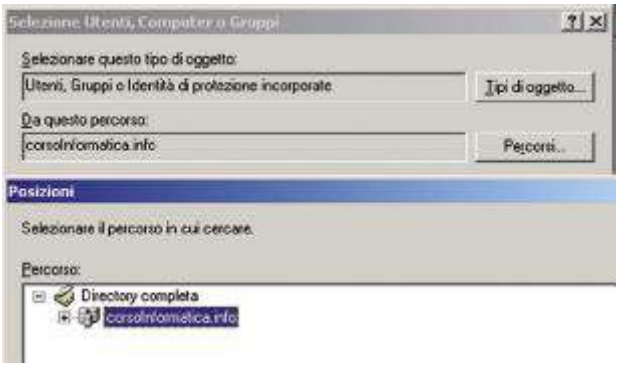
Vediamo come assegnare o modificare i permessi di accesso a una condivisione, per assegnare i permessi di condivisione a una cartella presente su di un volume formattato con FAT, FAT32 o NTFS.
Vediamo come aggiungere un utente alle autorizzazioni su una cartella.

Nel caso di NTFS dobbiamo assegnare all'utente anche le opportune autorizzazioni NTFS.

1. Quando siamo nella finestra di condivisione della cartella interessata entriamo nella voce Autorizzazioni e quindi facendo clic su Aggiungi appare la seguente finestra:

2. Facendo clic su Tipi di oggetto... possiamo scegliere il tipo di oggetto a cui associare l'autorizzazione (Computer, Gruppo o Utente):

3 Tramite Percorsi possiamo scegliere invece il dominio di cui ci interessa visualizzare gli utenti, i gruppi e i computers:



4 Possiamo a questo punto ricercare un utente scrivendolo nella casella Immettere i nomi degli oggetti da selezionare. Così se vogliamo cercare un utente che si chiama e.bianchi basterà scriverne il nome e fare clic su Controlla nomi per verificarne l'esistenza:

5 Se l'utente esiste appare il nome completo e possiamo procedere ad assegnare adesso le autorizzazioni di condivisione:

Zoom su...

CONDIVISIONI NASCOSTE

In Windows Server esistono alcune cartelle predefinite, utili all'amministratore e al funzionamento del sistema. Tali condivisioni sono caratterizzate dal fatto che il loro nome di condivisione termina con il simbolo $. Il simbolo impedisce che la condivisione venga visualizzata e la trasforma in una condivisione nascosta. Queste cartelle condivise vengono anche chiamate Condivisioni Amministrative.
Alcuni esempi di condivisioni nascoste sono tutte le unità logiche corrispondenti alle varie partizioni e volumi, la cartella di sistema, la cartella che contiene i drivers delle stampanti condivise, la condivisione utilizzata per i meccanismi di ◀ **interprocess communication** ▶ (IPC).

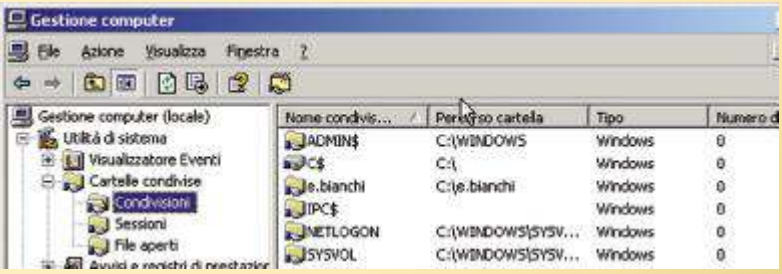
◀ Interprocess communication è il meccanismo che consente a diversi processi di comunicare tra loro scambiandosi dati e informazioni. I processi possono risiedere sullo stesso computer o essere distribuiti su una rete. ▶

Le condivisioni nascoste più importanti sono le seguenti.

- C$ Accesso alla partizione o al volume radice. Le altre condivisioni sono ugualmente accessibili dalla loro lettera, seguita dal carattere $.

- ADMIN$ Accesso alla cartella %systemroot%, che permette la gestione di una terminale sulla rete.
- IPC$ Permette la comunicazione tra i processi di rete. È possibile in ogni istante condividere ulteriori cartelle e fare in modo che siano condivisioni nascoste. Tali ulteriori condivisioni non risultano però essere delle condivisioni amministrative.
  L'unico modo per accedere a una condivisione nascosta è indicare per esteso il suo path, formato dal nome del server e seguito dalla condivisione:
  \\server\condivisione$
- PRINT$ Accesso da remoto alle stampanti.

Per visualizzare e gestire le condivisioni amministrative del computer, basta andare su Pannello di controllo / Strumenti di amministrazione / Gestione computer / Cartelle condivise / Condivisioni.

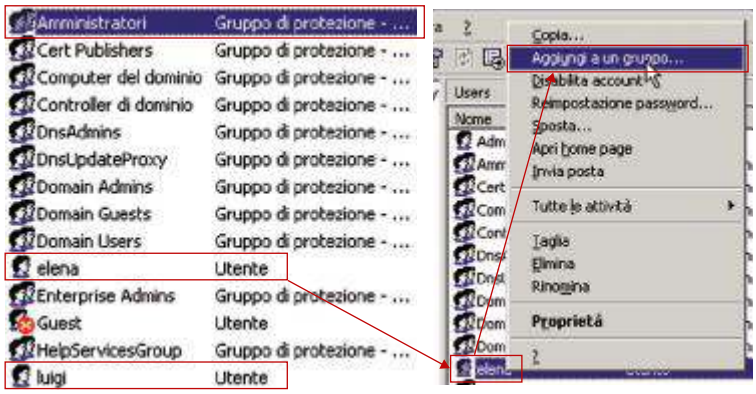


Tali condivisioni nascoste permettono all'amministratore di connettersi a qualsiasi partizione e volume di una macchina in modo tale da poter svolgere attività amministrative.

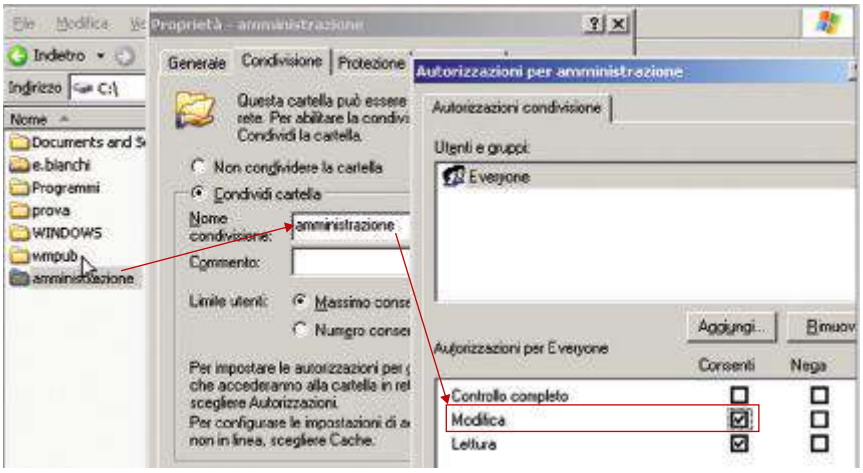
ESEMPIO

Condividiamo le cartelle in un file server

Per prima cosa andiamo a creare due utenti (luigi e elena) e li includiamo in un gruppo chiamato Amministrazione, come indicato dalla figura seguente:

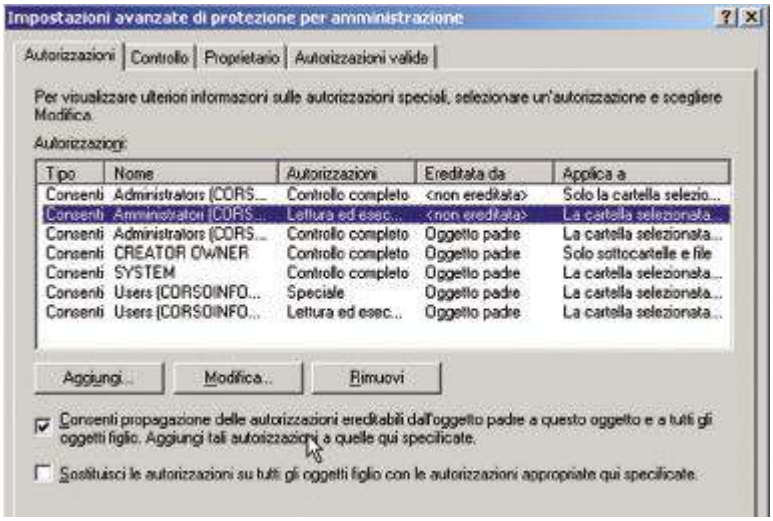


Adesso creiamo una cartella e la chiamiamo amministrazione. Dopo averla selezionata attiviamo il menu di condivisione e quindi la finestra Autorizzazioni.



Assegniamo alle autorizzazioni di condivisione i permessi di Everyone. Quindi passiamo adesso ad assegnare i criteri di protezione consentendo l'accesso solo al gruppo Amministratori, gruppo formato dagli utenti elena e luigi. ▶

Come possiamo notare il nostro dominio ha assegnato di default alcune autorizzazioni che dobbiamo tuttavia modificare. Facciamo clic sul pulsante Avanzate per modificare tali impostazioni:



Come possiamo notare appare nell'elenco anche il gruppo Amministratori. Dobbiamo quindi togliere la propagazione delle autorizzazioni ereditabili dall'oggetto padre per evitare di avere autorizzazioni non utili, per fare questo deselezioniamo la voce Consenti propagazione delle autorizzazioni...
Apparirà il messaggio della finestra a fianco in cui dobbiamo scegliere Rimuovi: ▶

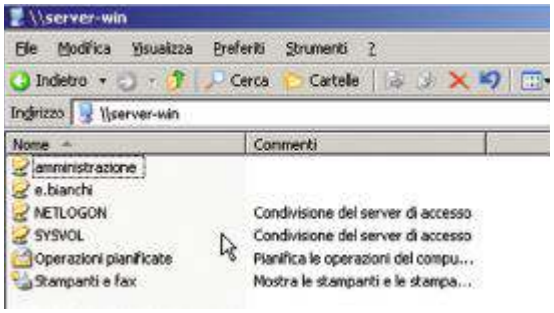
Come possiamo notare rimangono le sole autorizzazioni legate ai due gruppi Amministratori e Administrator, che consigliamo di lasciare per permettere all'amministratore di accedere a questa cartella da remoto: ▶

Se in questo riquadro apparissero altri gruppi di utenti o semplicemente utenti, andrebbero certamente eliminati premendo il tasto Rimuovi dopo averli selezionati.

Dopo aver confermato con OK dobbiamo indicare le autorizzazioni per il gruppo Amministratori. In questo caso lasciamo il controllo di Modifica ma non il Controllo Completo che preferiamo lasciare all'amministratore di sistema (gruppo Administrator): ▶

A questo punto per verificare che la cartella sia diventata una cartella condivisa facciamo clic su Start, quindi su Esegui digitiamo il nome del server (\\server-win) e facciamo clic su OK: ▼

Il risultato che otteniamo è quello che mostra la cartella condivisa Amministrazione a cui potranno accedere solo i membri del gruppo Amministrazione (elena e luigi): ▶



Prova adesso!

- Condividere una cartella
- Utilizzare un file server

1. Crea un utente per ciascuno dei tuoi compagni di classe e 4 gruppi (ad esempio Nord, Sud, Ovest e Est).
2. Crea 4 cartelle e assegnale ai 4 gruppi creati prima.
3. Adesso verifica che i compagni possano accedere da remoto solo alla propria cartella e che la cartella sia effettivamente condivisibile solo dagli utenti del gruppo di appartenenza.

CLIL

Server farm

A server farm or server cluster is a collection of computer servers, usually maintained by an enterprise to accomplish server needs far beyond the capability of one machine. Server farms often consist of thousands of computers which require a large amount of power to run and keep cool. At the optimum performance level, a server farm has enormous costs associated with it, both financially and environmentally. Server farms often have backup servers, which can take over the function of primary servers in the event of a primary server failure. Server farms are typically collocated with the network switches and/or routers which enable communication between the different parts of the cluster and the users of the cluster. The computers, routers, power supplies, and related electronics are typically mounted on 19-inch racks in a server room or data center. The image below shows one of Google's server farms in Council Bluffs, Iowa, which provides over 115,000 square feet of space for servers running services like Search and YouTube.

Directory service

A directory service is a network service that identifies all resources on a network and makes them accessible to users and applications. Resources include email addresses, computers, and peripheral devices such as printers. Ideally, the directory service should make the physical network topology and protocols transparent so that a user on a network can access any resource without knowing where or how it is physically connected. There are a number of directory services that are used widely. Two of the most important ones are LDAP, which is used primarily for email addresses, and Netware Directory Service (NDS), which is used on Novell Netware networks. Virtually all directory services are based on the X.500 ITU standard, although the standard is so large and complex that no vendor complies with it fully.

Basic network troubleshooting

Cause

A network may not work because of any of the below reasons.

1. Network or router connection issue card not connected properly.
2. Bad network card drivers or software settings.
3. Firewall preventing computers from seeing each other.
4. Connection related issues.
5. Bad network hardware.

Solution

Because of the variety of network configurations, operating systems, setups, etc. not all of the below information may apply to your network or operating system. Here it is not possible to provide assistance with network problems due to unknown passwords or unknown ISP settings.

Adapter resources

Verify that the network adapter is properly installed and detected by the computer with no conflicts. If you're using Microsoft Windows check in Device Manager and verify there are no errors and "Network adapters" is present with each network adapter installed in the computer listed, similar to the example on the right.

If conflicts exist or the network adapter is being detected as an "Other device", the network card has not been properly installed in the computer. Try letting Windows re-detect and install the Network card by removing the network adapter and any other conflict devices from Device Manager and then rebooting the computer. If Windows re-detects the card but does not find the drivers, download the network adapter drivers from the computer manufacturer or the network card manufacturer.

Verify connections

Wired Network: If this is a wired network, verify that the network cable is properly connected and make sure the LEDs next to the network jack are properly illuminated. For example, a network card with a solid green LED or light usually indicates that the card is either connected or receiving a signal. If the green light is flashing, this is an indication of data being sent or received. In the picture to the right, is an example of LAN port with two LED indicators next to the RJ-45 port. With this port, one LED will light up if connected properly and the other will flash when transmitting data. If there are no lights or the lights are orange or red the card may be bad, not connected properly, or the card may not be receiving a signal from the network. If you are on a small or local network and have the capability of checking a hub, switch, or router, verify that the cables are properly connected and that it has power. If after checking the connections the LED indicators appear bad, the network adapter, port, or cable may be defective.

Wireless Network: If you're using a laptop with a wireless network make sure, if the laptop has a Wi-Fi button, that it is turned on. Many laptops will have a Wi-Fi button that allows the wireless network to be turned on and off. In the picture to the right, is an example of a Wi-Fi button that is currently enabled. If the Wi-Fi button is turned on, make sure you're connecting to the correct Wi-Fi hotspot by right-clicking on the Network icon in the Windows notification area and clicking "Connect to a network". Usually, the network with the strongest connection (the most bars) will be your wireless router. Finally, when connecting to most wireless networks you will need to enter the proper SSID (password) in order to connect to the network. If the incorrect SSID has been entered you will be denied access to the network.

Adapter functionality

Verify that the network card is capable of pinging itself by using the ping command. Windows users can ping the computer from a Windows command line. Unix and Linux users can ping from the shell.
To ping the card or the localhost, type either

```
ping 127.0.0.1
```

or

```
ping localhost
```

Doing either of the above commands should get replies from the network card. If you receive an error or if the transmission fails, the network card is not physically installed into the computer correctly, has the incorrect drivers, or is bad.

Connect to the router

If all of the above steps have been checked and your network has a router, make sure the computer can connect to the router by performing the below commands.

Determine the router's address

Using the `ipconfig` command (or `ifconfig` command for Linux), determine the router's address by looking at the Gateway address. Below are the steps for Microsoft Windows users, Linux users can substitute `ipconfig` with `ifconfig`.

1. Open the Windows command line.
2. From the command prompt type ipconfig and press enter. This command should give you an output similar to the below example.

Ethernet adapter Local Area Connection:

```
Connection-specific DNS Suffix: computerhope.com.
IP Address ..................: 192.168.1.103
Subnet Mask .................: 255.255.255.0
Default Gateway .............: 192.168.1.1
```

The Default Gateway is the address of your router. Most home routers will have a gateway address that starts with 192.168 like the address shown above. Assuming your gateway address is 192.168.1.1, attempt to `ping` the router to see if it can send and receive information by running the below command.

```
ping 192.168.1.1
```

If you get replies back from the router, the connection between your router and computer is good, and you can move to the next step.

If you do not receive any replies back from the router, either the router is not set up properly or your connection between the router and the computer is not correct. Reset your router to make sure it is not a problem with your router by following the below steps.

1. Turn off the power to the computer and leave it off.
2. Unplug the power from your router and cable modem or DSL modem.
3. Leave the power cables disconnected for 10-15 seconds and then plug in your modem and then your router again.
4. Finally, turn on your computer again and repeat this step to see if you can ping your router.

If you're using a wireless network and have followed all the above steps and still are unable to ping the router, try turning off the computer again and connect the computer to the router using a cable instead of trying to connect using wireless. If using a cable does not fix it, either, contact the manufacturer of the router for additional support or replacement.

Firewall

If your computer network utilizes a firewall, make sure all required ports are open, especially port 80, which is the HTTP port. If possible, disable the firewall software program or disconnect the computer from the firewall to make sure it is not causing the network problems.

Internet is not working

If you're able to ping the router, but are still unable to connect to the Internet, either your router is improperly configured or the ISP is having issues.

Some ISPs such as Comcast require special software to be installed. Make sure any software included with your Modem or other hardware has been installed on at least one computer if you are setting up a new Internet connection.

If your Internet has been working but recently stopped working, give it a few minutes to make sure it is not a temporary outage. If after waiting a few minutes, you still have problems and you have not already disconnected the power from your router and modem follow the below steps.

1. Turn off the power to the computer and leave it off.
2. Unplug the power from your router and cable modem or DSL modem.
3. Leave the power cables disconnected for 10-15 seconds and then plug in your modem and then your router again.
4. Finally, turn on your computer again and repeat this step to see if you can ping your router.

If after following the above steps the Internet is still not working, open the Windows command line and run the below command.

```
ping google.com
```

Running the above command should get a reply from Google. If you get a reply, this is an indication that the Internet is working, but you may be encountering a problem with the Internet browser you are using to browse the Internet. Try an alternative browser such as Firefox or Chrome.
If you're getting no reply from Google, your router or modem is not reaching the Internet. If you have a router, make sure your router has DHCP enabled and that the WAN or Gateway address is the proper ISP address.
Finally, after verifying all of the above settings, if your Internet is still not working we suggest contacting the ISP to make sure it is not a problem on their end and to assist you further with any special configurations that may not be mentioned in this document.

Additional troubleshooting

Another method of determining network issues is to use the `tracert` command if you are a Windows user or the `traceroute` command if you are a Linux or Unix variant user. This command will give you an overview of each of the devices (routers) as a packet travels (hops) over a network and can give you an idea of where a problem exists in your network or outside of your network.
To use this command, you must be at the command line and type one of the commands below depending on your operating system.

```
tracert google.com
```

or

```
traceroute google.com
```

If run successfully, you should begin to see each hop between the computer and network devices. When the connection fails, determine what device is causing the issue by reviewing the traceroute listing.

LIBRO DIGITALE

VERSIONE
SCARICABILE
EBOOK

e-ISBN 978-88-203-7793-9

www.hoepliscuola.it
Ulrico Hoepli Editore S.p.A.
via Hoepli, 5 - 20121 Milano
e-mail hoepliscuola@hoepli.it